Optical Management System (OMS)

Release 6.3.4

Administration Guide

365-315-149R6.3.4
ISSUE 1
SEPTEMBER 2009

Legal notice

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Open Source Software

This product includes software developed by the following organizations and corporations:

- the Apache Software Foundation (http://www.apache.org/)
- cURL utility for transferring files created by Daniel Stenberg and can be found at http://curl.haxx.se
- the Castor Project (http://www.castor.org)
- JBoss
- the JDOM Project (http://www.jdom.org)
- Microsoft Corporation
- Netscape Communications Corporation
- the Open SSL project, by Eric Young and Tim Hudson
- qpthread, which was developed by Pravel Krauz
- the Samba Organization (http://www.samba.org)
- Sun Microsystems, Inc

Warranty

Alcatel-Lucent provides a limited warranty for this product. For more information, consult your local Alcatel-Lucent customer support team.

Ordering information

The ordering number for this document is 365-315-149R6.3.4. To order OMS information products, contact your local Alcatel-Lucent customer support team.

Technical support

For technical support, contact your local customer support team. You can reach them via the Web at the Alcatel-Lucent Customer Support web site (http://www. alcatel-lucent.com/support) or the customer support telephone number listed at the Alcatel-Lucent Contact Us web site (http://www.alcatel-lucent.com/contact).

Information product support

For questions or concerns about this or any other Alcatel-Lucent information product, please contact us at one of the following numbers: · (888) 727 3615 (for the continental United States) · +1 (630) 713 5000 (for all countries).

Contents

About this document

1 Administration Overview

2 Platforms

10 Backup, Recovery, and Restoration

11 Co-Resident and Distributed Architectures

15 One Vision Daily Log Extraction

16 Data Extraction

17 Northbound Support

20 Disaster Recovery

21 High Availability

22 Connection Auto Discovery

23 Network Inventory Extraction

24 Insert/Remove Node

25 NE In-Service Upgrade

26 1625 LambdaXtreme® Transport DWDM Upgrade and Merge

27 LambdaXtreme® Channel Upgrade

28 TDM NE Optical Lines Upgrade

29 CMISE NE Database Conversion

30 DMX/DMXtend NE Upgrade

31 NE Name Change

32 NE Reparenting

36 Bulk Renaming of Connections

37 Ethernet

38 Bulk Upload of Digital Link and Connections

39 Bulk Database Delete

40 Port Assignments

41 System Maintenance

42 Platform Alarms

43 Special Operations

A Tool Summary

About this document

Purpose

This preface provides an overview of this information product, which is the *Optical Management System Administration Guide*.

The purpose of this *OMS Administration Guide* is to explain to administrators how OMS is to be administered and maintained.

Reason for revision

Issue 1 of this *OMS Administration Guide* is a revised document that supports OMS Release 6.3.4.

Intended audience

This *OMS Administration Guide* is written primarily for operations personnel who administer OMS.

Safety information

This document does not contain any safety information or warnings because OMS is a software product.

How to use this information product

In the broadest sense, this *OMS Administration Guide* contains:

- *Conceptual* information, which is specific data related to the tasks
- *Task* information, which includes user tasks (that is, step-by-step instructions)

The conceptual information complements and enhances the step-by-step instructions that are found in each task. Use the conceptual information to broaden your general knowledge of the management system. It is best if you read all conceptual information and have a good understanding of the concepts being presented before undertaking the step-by-step instructions given in any task.

The task information is based on a user needs analysis that has been performed for each management system user job; therefore, use the task information to get the job at hand done quickly and with minimal system impact.

The conceptual and task information portions of the document have extensive hyperlinks. Use these links to toggle between the two types of information presented so you can access all pertinent information related to particular concepts and tasks.

This document can be used in its on-line versions (HTML/PDF) or in paper version (print PDF). The on-line HTML document version has a search capability, a full table of contents in the front matter of the document and a partial table of contents in each chapter, and an index for each document and for the entire management system library. Use all of these tools to help find information quickly. However, be aware that the index for each document in the management system library and the index for the entire management system library are the preferred search tools.

> **Important!** This document contains information on the complete line of network elements (NEs) that the OMS product supports. For a list of NEs that are supported in Release 6.3.4 of the management system, refer to the Summary of Supported NEs that is provided in Chapter 1 of this document.
>
> In addition, this document may contain information that is related to service packs (SPs) or maintenance releases that the OMS product is to support in the near future. This material may not yet be visible or operable on the management system servers and/or GUI and has been added only as a convenience for our OMS customers. This material is subject to change.
>
> This document supports the three hardware platforms on which OMS currently functions, which are the OMS HP® PA-RISC Server Platform (often referred to as the *Server Platform*), the OMS HP® Itanium® Server Platform (often referred to as the *Server Platform*), and the OMS PC Platform (often referred to as the *PC Platform*). Because the features that each platform supports vary, the variations of support are indicated in the text of this document where appropriate. In addition, the document library is offered on two CD-ROMs, depending on the platform on which OMS functions. Refer to “Related documentation”, which is in this section of the document for details regarding the two CD-ROMs that are available.

Conventions used

The conceptual information typically introduces each chapter or section of each chapter. The information presented in this area varies according to the topic being explained—sections, subsections, tables, figures, and screen captures can be commonly found.

The task information is presented as series of tasks that follows the conceptual information. These tasks are typically presented in the following functional order, depending on the nature of the subject being explained:

- *View a List of . . .*
- *View the Details of . . .*
- *Add . . .*
- *Create . . .*
- *Modify . . .*
- *Delete . . .*

Each task consists of sections that are called *When to use*, *Before you begin*, *Related information*, and *Task*.

The intent of the When to use, Before you begin, and Related information sections is self-explanatory—they explain when a task is to be used, what needs to be considered or done before you begin the task, and any related information that you would need to know while doing the task.

When a task does not have any conditions that must be considered before it is started, the Before you begin section for that task states: *This task does not have any preconditions.*

Each Task section consists of any number of steps. The completion of all steps, which are sequentially numbered, are required for the entire task to be completed successfully. In some instances, a step might be prefaced with the wording *Optional*, which indicates that the step can be skipped and the task can still be successfully completed. A task is considered to be completed when all of its steps are completed and when the wording **End of Steps** appears.

Many times, the management system affords the user with multiple ways to accomplish the same task. In these instances, one task can present the user with several **Methods** of how to accomplish the same set of steps successfully.

In addition, this *OMS Administration Guide* relies on the following typographical conventions to distinguish between user input and computer output.

- When describing the OMS software, fields in windows and field entries are identified with **this font**.
- When describing the UNIX® environment, text and numbers that the user inputs to the computer are identified with **`boldface type`**.
- In the UNIX® environment, text and numbers that the computer outputs to the user are identified with `monospace type`.

This *OMS Administration Guide* uses the following convention to indicate a *path* of pages that should be navigated through to arrive at a destination page:

- **Network > Submaps**

This same convention is also used to show a path through a series of menu items, for example:

- Click the filtering tool, and select **Node > Node Type**.

Occasionally, a set of management system features is not supported for all NEs or for both operating environments. This set of features is clearly marked to show these exceptions.

Related documentation

This *OMS Administration Guide* is part of a set of documents that supports OMS.

For the Server Platform, this document set is available on CD-ROM. The *OMS User Documentation CD-ROM* (365-315-144R6.3.4) includes the full set of documents listed below for the Server Platform in HTML and PDF formats.

Documentation

The document set that supports the OMS comprises the:

1. *OMS Getting Started Guide* (365-315-145R6.3.4), which instructs new users how to use OMS. This document contains a glossary of terms.
2. *OMS Network Element Management Guide* (365-315-146R6.3.4), which instructs users how to use OMS to provision and manage network elements.
3. *OMS Ethernet Management Guide* (365-315-147R6.3.4), which instructs users on how to use the Ethernet Management feature to provision and manage Ethernet connections in a network.
4. *OMS Service Assurance Guide* (365-315-148R6.3.4), which instructs users on how to manage and interpret fault information collected from the network.
5. *OMS Administration Guide* (365-315-149R6.3.4), which instructs users on how to administer and maintain OMS and the network.
6. *OMS Connection Management Guide* (365-315-150R6.3.4), which instructs users on how to provision connections and manage connections in the OMS and the network.

Help products

OMS includes an extensive help system that is designed to consider the task the user is performing and help that user successfully perform the task. The five help products described in the following table can be accessed from the Help menu on the top navigation bar of every page.

Help Product	Help Menu Item	Description
Task Help	**How do I ...**	Provides a list of tasks that can be performed from the current page. Clicking a task in the list presents the actual task. In addition, access is provided to the **Index**, which is the preferred search tool for the help system.

Help Product	Help Menu Item	Description
Page Help	**About this page**	Describes the purpose of the page, the toolbar tools, and a description of each field on the page. In addition, access is provided to the **Index**, which is the preferred search tool for the help system.
On-line Document Library	**On-line docs**	Presents the library of user documents, in both HTML and PDF formats. A search engine is included. *Note:* Access to the index of each document is provided. The index for the help system, which is the preferred search tool, is accessed from **How do I...**, **About this Page**, or **Technical Support** pages.
Technical Support Help	**Technical Support**	Provides technical support contact information. In addition, access is provided to the **Index**, which is the preferred search tool for the help system.
Product Help	**About OMS**	A pop-up window shows the version of the management system, along with links to the copyright and the OMS product pages. This page also contains information to acknowledge the open source software that OMS uses.

How to order

The ordering number for this document is 365-315-149R6.3.4. To order OMS information products, contact your local Alcatel-Lucent local customer service support team.

How to comment

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com) .

1 Administration Overview

Overview

Purpose

This chapter provides an overview of the OMS product and the system administration functions provided to maintain the OMS.

Contents

Product Overview

Definition

OMS is an integrated, modular system that offers a range of network element (NE), network connection, and service/order management functions. It links the management of traditional network equipment with next-generation technology and offers distribution options that can grow with network expansion. OMS controls service-restoration properties within the network, and complements this service-quality management with its own high-availability configurations.

OMS offers the benefits of fast service activation, state-of-the-art provisioning, reduced operating and equipment costs, accurate record keeping, fault management, and fast problem resolution. In addition, the management system can *discover* much of the information about NEs and network connections, instead of requiring that information to be entered manually, which minimizes network operator effort and reduces errors.

About the software

OMS is run through an Internet browser-based Graphical User Interface (GUI)—it is a *weblication* that runs through a browser. It supports the standard web features that a browser offers, such as bookmarks, back, forward, reload, and print.

In addition, the management system provides standard machine-to-machine interfaces so it can be easily integrated into the embedded operations environment of the service provider.

Support for both the SONET/SDH operating environments

The management system supports both the Synchronous Optical Network (SONET) and the Synchronous Digital Hierarchy (SDH) operating environments. The particular operating environment to be used is controlled by an installation parameter; refer to the "Default Terminology (SONET/SDH)" (p. 6-89) and "Terminology Choice" (p. 6-90) installation parameters for details.

User role profiles

When a user account is created, it is assigned a user role profile, which restricts the tasks the user login can perform. The management system offers these factory-defined user role profiles:

- NOC Administrator
- NOC Expert Operator
- NOC Operator

In addition, the management system allows the creation of a user-defined user role profile, which is a user role profile that consists of a customized list of tasks that is specific to the job responsibilities of the user.

Refer to “User Role Profile Concepts” (p. 7-2), “Factory-Defined User Role Profiles” (p. 7-3) , and “User-Defined User Role Profiles” (p. 7-5) in this document for details.

Installation parameters

An installation parameter is a parameter that is set during installation of the management system and may control the behavior of a feature.

Refer to Chapter 6, “The Application and Its Installation Parameters” in this document for details.

User Activity Log

All provisioning changes done using the management system are logged in the User Activity Log. For detailed information about the User Activity Log, refer to the *OMS Network Element Management Guide*.

Although it is not stated as part of the results for every task in this document, you can assume that all tasks that result in an administration change are logged to the User Activity Log.

Licensable Features

Optional Server Cores for Distributed Configuration

The following are optional licensable Server Cores for Distributed Configuration (single license on each server) in addition to the main OMS server.

- OMS R6.3 Bulk PM Server
- OMS R6.3 Network Adapter
- OMS R6.3 GUI WEB Server

Optional Features

The following are optional features which can be licensed.

- OMS R6.3 (HP® rp3410) Intelligent Routing
- OMS R6.3 (HP® rp3440) Intelligent Routing
- OMS R6.3 (HP® rp3410) Enhanced Ethernet provisioning
- OMS R6.3 (HP® rp3440) Enhanced Ethernet provisioning
- OMS R6.3 (HP® rp3410) Geographic Domain Partitioning

- OMS R6.3 (HP® rp3440) Geographic Domain Partitioning
- OMS R6.3 COMPACT Root Cause Failure Analysis
- OMS R6.3 (HP® rp3410) Root Cause Failure Analysis
- OMS R6.3 Root Cause Failure Analysis
- OMS R6.3 Distributed Bulk PM interface
- OMS R6.3 Pre-Plan Restoration

Operation Interfaces

The following are optional operation interface features which can be licensed.

- OMS R6.3 COMPACT NB ASCII for Alarms (TIM)
- OMS R6.3 (HP® rp3410) NB ASCII for Alarms (TIM)
- OMS R6.3 (HP® rp3440) NB ASCII for Alarms (TIM)
- OMS R6.3 COMPACT NB SNMP (FM)
- OMS R6.3 (HP® rp3410) NB SNMP (FM)
- OMS R6.3 (HP® rp3440) NB SNMP (FM)
- OMS R6.3 Data Extraction Tool
- OMS R6.3 VPI Network Inventory Extraction Tool
- OMS R6.3 NB TMF814
- OMS R6.3 NB MTOSI (JBoss-MQ)

High Availability features

The following are optional high availability features which can be licensed.

- OMS R6.3 Disaster Recovery Base per server
- OMS R6.3 ATT HOTDR per server

Supported Network Elements

The management system and its supported NEs

OMS supports Alcatel-Lucent's family of optical NEs. To accommodate the world of optical transmission standards, these Alcatel-Lucent NEs operate using different transport structures and they support different native command languages. Refer to "Summary of supported NEs" (p. 1-5) for a list of the particular NEs and the releases of those NEs that the management system supports.

The SDH and SONET transport structures

Alcatel-Lucent's NEs are designed to operate in the Synchronous Digital Hierarchy (SDH) operating environment, the Synchronous Optical Network (SONET) operating environment, or both environments. Refer to "Summary of supported NEs" (p. 1-5) for a list of the transport structure of each supported NE.

The TL1 and CMISE native command languages

Each NE supports a native command language that is used to control the NE at the network-element-level via the Command Interface Terminal (CIT).

The management system supports NEs that are controlled with the following two different native command languages:

- TL1, which is Translation Language 1
- CMISE, which is Common Management Information Service Element

The management system uses the native command language of the NE to implement some of its features; consequently, differences in management system behavior can be attributed to one native command language or another, which is why this categorization is significant. Therefore, throughout this document, references are made to *TL1 NEs* or *CMISE NEs*.

Refer to "Summary of supported NEs" (p. 1-5) for a list of the native command language of each supported NE.

Summary of supported NEs

The following table summarizes each supported NE and its release, along with its transport structure and its native command language.

Important! Each release of OMS supports certain NEs within Alcatel-Lucent's family of optical NEs. Mention of NEs or specific NE features in the text of this document that are not supported in this particular release of the management system apply to prior releases of the management system. Such material may not be currently visible or operable on the management system GUI and has been added only as a convenience for our OMS customers.

NE Supported[1]	NE Release Supported	Transport Structure Supported	Native Command Language Supported	Transmission Technology
ISM ADM 1	R2.5[4] R3.5[4]	SDH	CMISE	TDM
ISM ADM 4	R2.5[4] R3.5[4]	SDH	CMISE	TDM

NE Supported[1]	NE Release Supported	Transport Structure Supported	Native Command Language Supported	Transmission Technology
ISM Repeater 1	R2.5[4] R3.5[4]	SDH	CMISE	TDM
ISM Repeater 4	R2.5[4] R3.5[4]	SDH	CMISE	TDM
ISM TM 1	R2.5[4] R3.5[4]	SDH	CMISE	TDM
ISM TM 4	R2.5[4] R3.5[4]	SDH	CMISE	TDM
1675 Lambda Unite MultiService Switch (MSS)	R10.5.4 R10.5.3 R10.5.2 R10.5.1 10.5 R10.0 R9.1 R9.0 R8.0.20 R7.0.2 R6.1.1	SONET / SDH	TL1	TDM
1625 LambdaXtreme® Transport	R9.0 R8.1 R7.0, R6.0 R5.1.1 R5.3.2	SONET / SDH[2]	TL1	DWDM
1643 ADM MultiService Mux (Compact Shelf)	R5.0.3 R3.1 R3.2 R3.3 R3.0[4]	SDH	CMISE	TDM

NE Supported[1]	NE Release Supported	Transport Structure Supported	Native Command Language Supported	Transmission Technology
1663 Add Drop Multiplexer (ADMu)	R6.1 R6.0 R5.2 R5.1 R5.0.3 R4.0.4	SDH	CMISE	TDM
1643 Access Multiplexer (AM)	R7.2.1 R7.1 R6.1H R5.0D R3.0 R3.1 R3.2[4] R2.2[4]	SDH	CMISE	TDM
1643 Access Multiplexer Small (AMS)	R7.2.1 R7.1 R6.1H R5.0D	SDH	CMISE	TDM
1655 Access Multiplexer Universal (AMU)	R5.0 R4.1.1 R4.0 R3.0 R2.1 R2.0.4	SDH	CMISE	TDM
1665 DMX Access Multiplexer	R8.0.1 R7.1.1 R7.1 R7.0.x R6.0.x R5.1.x	SONET	TL1	TDM
1665 Data Multiplexer Explore (DMXplore)	R2.1	SONET	TL1	TDM

NE Supported[1]	NE Release Supported	Transport Structure Supported	Native Command Language Supported	Transmission Technology
1665 DMXtend Access Multiplexer	R8.0.1 R5.1.1 R5.1 R5.0.x R4.0.x R3.1.x	SONET	TL1	TDM
1694 Enhanced Optical Networking (EON)	R8.8 R8.6.3 R8.4.1	SONET / SDH[2]	TL1	DWDM
1695 Wavelength Services Manager (WSM)	R6.0 R5.0 R4.5 R4.0 R3.0	SONET / SDH[2]	TL1	DWDM
PHASE ADM 4/4	R5.0[4]	SDH	CMISE	TDM
PHASE ADM 16/4	R5.0[4]	SDH	CMISE	TDM
PHASE LR 4	R5.0 [4]	SDH	CMISE	TDM
PHASE LR 16	R5.0 [4]	SDH	CMISE	TDM
PHASE LXC 4/1	R5.0 [4]	SDH	CMISE	TDM
PHASE LXC 16/1	R5.0[4]	SDH	CMISE	TDM
PHASE TM 4/4	R5.0[4]	SDH	CMISE	TDM
PHASE TM 16/4	R5.0[4]	SDH	CMISE	TDM
SLM ADM 16	R5.0[4]	SDH	CMISE	TDM
SLM MS Protected TM 4	R5.0[4]	SDH	CMISE	TDM
SLM MS Protected TM 16	R5.0[4]	SDH	CMISE	TDM
SLM Regenerator 4	R5.0[4]	SDH	CMISE	TDM
SLM Regenerator 16	R5.0[4]	SDH	CMISE	TDM
SLM Unprotected TM 4	R5.0[4]	SDH	CMISE	TDM
SLM Unprotected TM 16	R5.0[4]	SDH	CMISE	TDM
WaveStar® ADM 4/1	V5 R4[4]	SDH	CMISE	TDM

NE Supported[1]	NE Release Supported	Transport Structure Supported	Native Command Language Supported	Transmission Technology
WaveStar® ADM 16/1	R8.0.3 R7.0.1 R6.2.5[4] R6.1, R6.0[4]	SDH	CMISE	TDM
WaveStar® AM 1	R3.1[4]	SDH	CMISE	TDM
WaveStar® Bandwidth Manager	R4.1.6[3, 7]	SONET	TL1	TDM
WaveStar® DACS 4/4/1	R3.1[4] R3.0[4]	SDH	CMISE	TDM
WaveStar® OLS 1.6T	R11.0 R10.0 R9.0[7] R8.0[3, 7] R7.1[6, 7] R6.2.2[6, 7]	SDH	TL1	DWDM
WaveStar® TDM 10G (STM64)	R5.0[5, 7] R4.0 [5]	SDH	TL1	TDM
1645 Access Multiplexer Compact (AMC)	R9.0 R8.0	SDH	CMISE	TDM

[1] Also supports the Unknown NE type, the Non-managed NE, and the Unmanaged Device.

[2] Carries SONET/SDH transparently.

[3] Releases listed are supported via cut-through to Navis® EMS R10.3.2. Domain and network level support is also provided via the EMS G7 interface by the management system's OMS GUI.

[4] Release listed is supported via cut-through to ITM-SC R10.2 and NE is considered to be indirectly managed. Domain and network level support is also provided by the management system's OMS GUI via the XML interface between ITM-SC and the management system.

[5] Releases 5.0 and 4.0 are supported directly by OMS R6.1. Release 5.0 is also supported indirectly via Navis® EMS R10.3.1.

[6] Releases listed are supported via cut-through to Navis® EMS R10.3.1.

[7] Releases listed are supported via cut-through to Navis® EMS R10.3.4

Security Management

Industry standard security features

The OMS supports industry-standard security functions. The base security layer of the OMS is provided by the HP-UX® operating system platform, which provides a secure computing environment. The middle security layer supplies the application-specific security management functions, such as executing user work-function permissions. The top security layer provides management system-based access for the administrator of the management system to manage the application-level security functions.

The administrator of the management system, who is referred to as the NOC administrator, performs all system security measures through the security screens of the management system user interface. Discretionary access is implemented through access control structures at the application and workstation layers. Central access to all security functions is provided through the management system.

Security features supported include the following:

- User login authentication
- User inactivity timeout
- Enable/disable user logins
- Assign user role profiles
- Acceptance or decline of a proprietary warning message

User authentication and authorization

The NOC Administrator is equipped with tools to add, manage, change, and delete authorized users on the management system. Each user has a unique login and password, and the system tracks active users.

The management system enforces password complexity, including length and alphabetic/numeric composition. When authentication fails, the only information that the management system supplies to the user is that the user attempt was invalid.

In addition, the management system requires proper identification and authentication every time communications to a user is reinstated. For example, if users are timed out, they must regain authentication and authorization. Users accessing the management system console cannot gain access to the management of network equipment.

User passwords are transferred in encrypted form from the management system to the HP® server and are stored in encrypted format.

End-to-end authentication and authorization

OMS provides security over its southbound interfaces to the NE by supporting global password administration for the NE login IDs used by OMS. Global password administration enables administrators to change the passwords used by the management system for many NEs quickly and easily in a single operation.

HTTPS/SSL protocol support

Because the management system uses the HTTPS/SSL protocol, security warnings are displayed to users upon their login into the management system. Refer to "Security warnings displayed to users" (p. 8-5) for more information on how users are to proceed with their logins and the "Eliminate Security Warnings upon User Login" (p. 8-25) task for how to disable these warnings.

OMS created logins

OMS creates default administrator logins for its various operating environments. It is the administrator's responsibility to immediately change the default passwords that accompany these logins to a meaningful, yet relatively obscure, password. Refer to "Administrator logins and passwords" (p. 1-13) for details on the various operating environments.

Domain Partitioning Management

Domain Partitioning definition

Domain Partitioning Management is the ability to allocate NEs to domains and to restrict a user's access based on the domain. With Domain Partitioning Management, a network operating company can partition its network hierarchically by its organizational structure or its geographical regions.

Domain Partitioning license

Domain Partitioning Management is an optional, licensable feature that is only available to customers who have purchased the feature and installed its license.

The successful operation of Domain Partitioning Management requires the "OMS_DP license" (p. 5-6) license. Feature licenses are typically installed, and thereby activated, upon the installation of the management system. Any subsequent additions of licenses require the license key and are made with the "Add a License" (p. 5-18) task.

Domain categories

A domain is a logical association of network resources and users. The network resources include entire NEs and the domain users include Domain Administrators and Domain Operators.

The two categories of domains are the following:

- A *global domain* is created automatically when the "OMS_DP license" (p. 5-6) is installed. The entire network that is managed under OMS is considered to be a global domain and all management system users are domain users. Network resources and users who lie in a global domain can be assigned to user-created domains.
- *User created domains* are those domains that are created, modified, and deleted manually. User created domains are associate a set of users with a set of network resources.

When a domain is created, the existence of users and network resources residing in the domain are optional; a domain can exist with only users, with only network resources, or with neither users nor network resources.

Domain users

When user accounts are created, users can be assigned to a **Non-restricted** or **Restricted** domain:

- A **Non-restricted user** is associated with the global domain.
- A **Restricted user** can be allocated to any user-defined domains, but a restricted user cannot be associated with the global domain.

Domain hierarchies

Domains can be arranged into multi-level parent/child/grandchild/...hierarchies.

The global domain is a parent or grandparent of all domains. Any domain can have multiple children; however, a child domain can only have one parent.

A parent domain can view and manage all network resources that are contained in its children/grandchildren/...domains.

Administrator Logins, Passwords, and Privileges

The operating environments of the OMS administrator

The OMS administrator operates in the following environments:

- The *Command Line Man Machine Interface (CLMMI)* environment, which supplies a text-based user interface. This interface supports UNIX® and/or Windows® 2000 or Windows® XP system administrators who need access to the command line of the operating system. The CLMMI environment enables administrators to start and stop applications, to run command-line tools, or to view surveillance logs.
- The *web-based interface* to the management system, which supplies a graphical user interface. This *weblication* supports system administrators operating in the Windows® environment who need access to the pages of the management system to add licenses, create user role profiles, create user accounts, and perform hot-backup functions. **Note:** Because these system administrators require a **NOC Administrator** user role profile, they are often referred to as *NOC Administrators*. See "User role profile needed" (p. 1-14) and "Privileges" (p. 1-15) for details.

Administrator logins and passwords

Because the OMS administrator performs tasks in several operating environments, the following logins and passwords are required to ensure accessibility to all tasks and functions:

- A **root** login and password are required to access the device on which the management system is running and to restart this device, to execute some command-line tools, to create the proprietary agreement for the management system, and to run a cold backup. Note: The installer initially enters the root password when prompted by the installation process. It is the administrator's responsibility to change the default password that accompanies the root login to a meaningful, yet relatively obscure, password.
- On the Server Platform and PC Platform, an **oms** login and password are required to access the administration functions of the OMS that are performed at the command line, such as starting and stopping the management system application or viewing the error trace logs. It is the administrator's responsibility to change the default password that accompanies the **oms** login to a meaningful, yet relatively obscure, password.
- On the PC Platform, an **omsgui** login is required to launch the Firefox browser on the Linux® server.
- An **oracle** login and password are required on the HP® servers for database administration. It is the administrator's responsibility to change the default password that accompanies the **oracle** login to a meaningful, yet relatively obscure, password.
- A **tna** login and password are required if the TL1 network adapter is installed on the server for TL1-related administration. It is the administrator's responsibility to change the default password that accompanies the **tna** login to a meaningful, yet relatively obscure, password.

- A **nma** login and password are required if the NMA network adaptor is installed on the server for 1671 Service Connect (SC) related administration. It is the administrator's responsibility to change the default password that accompanies the **nma** login to a meaningful, yet relatively obscure, password.
- A **cna** login and password are required if the CMISE network adapter is installed on the server for CMISE-related administration. It is the administrator's responsibility to change the default password that accompanies the **cna** login to a meaningful, yet relatively obscure, password.
- A **bpm** login and password are required if Bulk Performance Monitoring (BPM) is installed on the server. It is the administrator's responsibility to change the default password that accompanies the **bpm** login to a meaningful, yet relatively obscure, password. Refer to "BPM" (p. 11-6) for details.
- A NOC Administrator login and password are required for access to the OMS. The NOC administrator can then administer management system licenses, user accounts, user role profiles, and system backups.

  The user name for this account is set to **adminusr**; this factory-defined name cannot be changed. The adminusr account cannot be suspended or deleted. The locked out threshold of three consecutive invalid login attempts does not apply to the **adminusr** account. In addition, the **Suspend user**, **Delete user**, and **Activate user** Go menu items do not apply to the **adminusr** account.

  The initial password for the adminusr account is set to **adminusr**; this password must be changed after the NOC Administrator has initially logged in as adminusr. The **adminusr** password must be changed when the value set for the password aging installation parameter has expired; refer to the "Password Aging Time" (p. 6-121) installation parameter for details.

  Important! When two users log in to the management system as **adminusr**, the second user can kill the session of the first user if the checkbox for `Click here to close the previous session` on the login page is selected. If the first user's session was manually killed while that user was sending a data request, the management system might not display any data to that user because the session was invalidated.
- Any other administrator login and password needed to administer any third-party software running on the Windows® 2000 or Windows® XP PC or the HP® servers are also required.

  Important! Administrator privileges on the PC are needed in order to run the AutoConfig.jsp tool and to install the Java plug-in.

User role profile needed

Initially, administrators of the management system have the user role profile of **NOC Administrator**, which is the factory-defined user role profile. If needed, administrators can easily combine administrative functions and advanced user functions by creating a user-defined user role profile. Refer to Chapter 7, "User Role Profiles" for details.

Privileges

NOC Administrators are assigned privileges that enable them to create, modify, or delete any class of user, and to set up user role profiles. However, the NOC Administrator password is subject to aging restrictions.

Note: the privileges afforded to the NOC Administrator do not map to the UNIX® superuser (the **root** login).

Management System Databases

Types of management system databases

The OMS relies on the following databases to store pertinent information:

- The OMS database (OMS database) stores information relative to the network and element layers of the management system.
- Lightweight Directory Access Protocol (LDAP) database stores information relative to user management, such as user accounts created.

Database synchronization process

The system administrator must use a *database synchronization* process to synchronize the OMS database with the databases for the particular network elements (NEs) that are being monitored. Database synchronization is a management system process in which NE alarms and configuration information are collected and stored in the management system database. Database synchronization should be performed before any database backed up is attempted; refer to the *OMS Network Element Management Guide* and/or the *OMS Ethernet Management Guide* for details.

Backup of the databases

The system administrator is responsible for running hot and cold backups on the database. Refer to “Types of system backups” (p. 10-2), “Run cold system backups” (p. 41-2), and “Run hot system backups” (p. 41-1) for details.

General Order of Administration

The roadmap

For the administration process to go as smoothly as possible, the OMS team offers new administrators of the management system the following roadmap:

1. Verify that the installation of the HP® server hardware for the Server Platform and the PC hardware for the PC Platform is completed and that all hardware is up and running.
   Account for all documentation received with the hardware and ensure its accessibility. Acquaint yourself with this documentation.
2. Secure the needed administrative logins/passwords for the HP® server, the Windows® 2000 or Windows® XP PC, the management system, and the operating environments associated with which the management system is associated. (Refer to "Administrator logins and passwords" (p. 1-13) for a list of the operating environments.)
   Change the default password that accompanies each login to a meaningful, yet relatively obscure, password.
3. Before you actually begin to use the management system, acquaint yourself with the nature of the alarms that might appear at any time, and consequently might have to be reconciled, on the HP® server. These alarms are referred to as *Platform Alarms*.
   Refer to "Alarm Classifications" (p. 42-1) and "List of Platform Alarms" (p. 42-7) in this guide. For a more complete explanation of alarms, refer to the *OMS Service Assurance Guide*.
4. Verify that the HP® server software and the client operating system are installed and are up and running. If the configuration is on the OMS PC Platform, verify that the software is installed and up and running.
   Account for all documentation received with the software and ensure its accessibility. Acquaint yourself with that documentation.
   Refer to "HP® Servers Software Platform" (p. 2-1) and "Client software platform" (p. 2-4).
5. If you did not log into the management system for the first time in the previous step, log in to the management system using the "Log in to OMS for the First Time" (p. 3-33) task as **adminusr** using the **adminusr** password. Immediately, change the **adminusr** password to a password that is meaningful and secure to you, the NOC Administrator.
   Refer to the "Log in to OMS for the First Time" (p. 3-33) task or to the *OMS Getting Started Guide* for instructions on how to log in to the management system. Refer to the *OMS Getting Started Guide* for instructions on how to change a password. Refer to "User ID Rules" (p. 8-9) and "Password Rules" (p. 8-11) in this guide for a details on the limitations imposed on user IDs and passwords. (Note: If you want to customize a user role profile for yourself at this time, go to last part of Step 9.)

6. Set up the administration and user PCs/clients, which involves verifying that software versions and, if need be, installing and or changing parameter settings regarding the PC control panel, Microsoft® products, and the Java™ Plug-in.
   Refer to and complete all tasks in Chapter 3, “Client Set Up”.
7. Verify that the various licenses purchased to run the management system are installed and that the features that are indicative of each license are operational.
   Refer to “The Management System and Its Licensing Function” (p. 5-1).
   Besides feature activation, licenses are used to activate a variety of command-line tools that are available to the system administrator who has **root** or **oms** login privileges. Refer to Chapter 16, “Data Extraction”, Chapter 18, “TMF814 Northbound Interface”, and Chapter 23, “Network Inventory Extraction”.
   If a particular license has not been installed, contact your Alcatel-Lucent local customer service support team or your installer.
   Once you have the information needed to activate the license, use the “Add a License” (p. 5-18) task.
8. Familiarize yourself with user role profiles and determine the access needs of your user community and the security constraints to be imposed at your installation.
   If necessary, survey the user community to determine their access needs and the management community to determine security constraints.
   Refer to Chapter 7, “User Role Profiles”.
   If Domain Partitioning Management is installed for a particular site, carefully review the “Domain Partitioning Management” (p. 1-11), “Domain Administration user task” (p. 7-10), and “OMS_DP license” (p. 5-6) sections in this document before making any user role profile assignments.
9. Add any new users who are to use the factory-defined user role profiles immediately.
   Refer to the “Add a User Account” (p. 8-15) task.
   For those new users who need customized user role profiles, create any user-defined user role profiles before the users are added. Refer to the “Add a User-Defined User Role Profile” (p. 7-25) task.
   In addition, create a user-defined user role profile for yourself, the NOC Administrator, that will allow you to access all areas of the management system. For example, as the name *alltasks* implies, this user-defined user role profile would include all tasks provided. Refer to the “Add a User-Defined User Role Profile” (p. 7-25) task.
   Refer to “Creation of user-defined user role profiles” (p. 7-5).
10. After a considerable amount of user data has been added to the management system, perform a database synchronization and backup the database.
    Refer to the *OMS Network Element Management Guide* for details on how to perform a database synchronization. Refer to “Types of system backups” (p. 10-2), “Execute an Immediate Hot System Backup from the OMS” (p. 10-8) , and “Execute a Cold System Backup from the HP® Server” (p. 10-9) for details in this guide on database backups.

11. As you become comfortable with and knowledgeable of the system, you **might** need to tune some of the various installation parameters to accommodate the particular needs of the site. Refer to Chapter 6, “The Application and Its Installation Parameters”, “lt_param_reconfig and its menu options” (p. 6-3), and “Installation Parameters and the Proprietary Agreement” (p. 6-164) before you attempt to change these parameters.
    Once you are confident of what you want to change, refer to the appropriate task: “Modify an Installation Parameter” (p. 6-167) or “Create a Customized Proprietary Agreement” (p. 6-168). Beware that some installation parameter modifications require the application to be stopped.
12. After the system is up and running, become aware of the system maintenance that must be performed regarding the management system and the platform on which the management system runs. Refer to “Daily Housekeeping” (p. 41-1) and “Periodic Maintenance” (p. 41-2) for details.

2 Platforms

Overview

Purpose

This chapter provides a detailed explanation of the software platform that OMS supports.

Contents

HP® Servers Software Platform

HP® server required software

The following table lists the software components that are required for the management system server, which include the HP-UX® operating system with accompanying bundled software plus other open source software.

Software Component	Version
HP-UX® Operating System	11.23
Oracle® Standard Edition	10.2.0.3
Orbix® ASP Standard/Enterprise Edition	6.3_SP3

HP® server open source software

The following open source software is installed with the management system application and is run in conjunction with the HP® server platform and/or the management system.

Open Source Software Installed Along with the Management System Application
Apache web/application server software
ATOS
commons-codec
commons-collections
commons-logging
commons-fileupload
commons-io
Curl command line tool for transferring files
HttpCient
JAVA Plug In
JAXP UI library/visualization software
JBoss Message Queue (in MTOSI)
JDK
JiBX
jsch
jta
LDAP
log4j
Microsoft® Internet Explorer web browser*
OpenSSL
Perl scripting software required by Apache
piccolo.jar
qpthread
SNMP4j
ssh
Tomcat web/application server software
Xalan UI library visualization software
Xercesc

Open Source Software Installed Along with the Management System Application
Important! *The script scan feature of McAfee VirusScan 8.0.0 (Enterprise), patch levels up to 10, might cause an IE browser that is running any release of the management system GUI to crash. If McAfee VirusScan 8.0.0 is installed, then (up to) patch 11 must be installed to avoid this problem.

HP® server Disaster Recovery required software

The following table lists the software components that are required for the management system server if the Disaster Recovery feature is installed.

Software Component	Version
Veritas® Volume Manager (Disk Mirroring and Disaster Recovery)	4.1
Veritas® Volume Replicator (Disaster Recovery)	4.1

HP® PA-RISC Server Serviceguard required software

The following table lists the software component that is required for the management system server if Serviceguard is installed on a PA-RISC server.

Software Component	Version
HP® Serviceguard	a.11.17

Client Platform

Client hardware platform

The client includes the following hardware components and peripherals:

- A monitor, keyboard, mouse, network interface card (NIC), CD-ROM or DVD-ROM drive, and a floppy disk drive are required.
- A sound card and speakers are required for audible notification of alarms.
- A printer should be included if a printout of viewed pages is required.

Since the management system uses a web browser paradigm, the *GUI client* can run on any *IBM-PC compatible* type of system that supports the operating system/browser combination and has sufficient free resources (for CPU, RAM, disk, video resolution).

We provide the following client recommendations:

- A specification without a legacy element management system (EMS) (SC/SNMS) GUI access feature.
- A specification with a legacy EMS GUI access feature.

If other applications are to be run with the management system, additional memory is required; the exact amount of memory depends on the particular applications.

The following table lists the components and specifications of the client configuration with or without access to an EMS GUI. The "Verify the OMS Client Hardware Configuration" (p. 4-9) task can be used to verify the correct hardware configuration.

Component	Specification with out EMS GUI Access	Specification with EMS GUI Access
Pentium™ 4 CPU	1.8 GHz	1.8 GHz
RAM	512 MB	1 GB (additional 256 MB for each additional EMS GUI)
Disk Space	2 GB (7200 RPM EIDE)	2 GB (7200 RPM EIDE)
Video Capability	24-bit color, 1280 x 1024 pixels	24-bit color, 1280 x 1024 pixels
Video RAM	8 MB	8 MB
Color Monitor	21 inch	21 inch
Virtual Memory	1 GB	1 GB

Client software platform

The following table lists the components and versions of the client software platform for the management system.

Software Component	Type and Version
Operating System	Windows® 2000 Professional, Service Pack 3 or higher
	Windows® XP Professional, Service Pack 1 or higher
Browser*	Internet Explorer® 6 Service Pack 1 (SP1)*
Plug-in**	Java™ Run-Time Environment J2SE v. 1.6.0_02***
Other	DirectX® R9.0

<table>
<tr><th>Software Component</th><th>Type and Version</th></tr>
<tr><td colspan="2">* Because the management system relies on pop-up windows, any type of pop-up inhibiting software that runs in conjunction with the browser must be disabled while running the management system.
Important! The script scan feature of McAfee VirusScan 8.0.0 (Enterprise), patch levels up to 10, might cause an IE browser that is running any release of the management system GUI to crash. If McAfee VirusScan 8.0.0 is installed, then (up to) patch 11 must be installed to avoid this problem.
** The Java™ Plug-in version scheme used is of a static nature, which means that it is automatically installed so it is compatible with management software.
*** Multiple JRE versions often cannot co-exist; and, when multiple JRE versions are present, the management system GUI might not function properly.</td></tr>
</table>

3 Client Set Up

Overview

Purpose

This chapter provides instructions on how to set up the client in order to run the OMS.

Contents

Important Information about the Client Set Up

Software that must be installed

The following software must be installed on the client before the it can be used to access the OMS web site:

- Windows® 2000 Professional with Service Pack 3 (SP3) or higher, or Windows® XP Professional with SP1 or higher.
- Microsoft® Internet Explorer (IE) 6 or 7.
  OMS does not support operation on any version of Netscape® Navigator.
  Important! The script scan feature of McAfee VirusScan 8.0.0 (Enterprise), patch levels up to 10, might cause an IE 6 browser that is running any release of the management system GUI to crash. If McAfee VirusScan 8.0.0 is installed, then (up to) patch 11 must be installed to avoid this problem.
  Special configuration tasks are required for an IE 7 browser. See “Microsoft® IE 7.0 Considerations” (p. 3-4) for details.
- DirectX® application programming interface Version 8.1 or higher for Windows® 2000 Professional with Service Pack 3 (SP3).
  Important! Windows® XP Professional with SP1 is bundled with the DirectX® application programming interface Version 8.1; therefore, Windows® XP users do not have perform the associated DirectX® task provided in this documentation.
- Java™ 2 Runtime Environment 1.6.0_02, which is also known as the Java™ Plug-In.
  Important! Previous JRE versions cannot co-exist with JRE version 1.6.0_02. If both JRE versions are present, the management system GUI does not function.
- A tool required to view PM data that appears in tab separated files, such as Microsoft® Excel or its equivalent.

Two methods of client set up

The following two methods of installation are available for client set ups:

- *Automatically* via the Auto Configuration tool, which is the preferred and recommended method; see the “Run the Auto Configuration Tool for the Client Set Up” (p. 3-6) task.
- *Manually* via a series of tasks that are provided.

Critical order of software installation and set up

When setting up the client manually, the order in which the software is verified and/or installed or set up must match the order in which the task and the steps for each task are presented in this document. The order of installation is critical because if one piece of software is installed or set up before the other problems can occur.

For example: the critical nature of the order in which tasks must be performed is most evident in the tasks supplied for the Java™ Plug-in in which the version of the Java™ Plug-In that is current on the client must be verified, and if need be, the incorrect version of the plug-in must be uninstalled and the correct version of the plug-in must be reinstalled, before the management can be run.

Types of tasks involved when manually setting up the client

In general, the tasks that need to be performed when manually setting up the client involve verifying software versions and, if need be, installing and/or changing parameter settings regarding the following:

- PC Control Panel, which include specific tasks for virtual memory size, polling sounds, pop-up inhibiting software, and font sizes.
- Microsoft® products, which includes specific tasks for the Service Pack, Microsoft® IE, and DirectX® application programming interface.
- Java™ Plug-in, which includes specific tasks for the Plug-In and its Runtime Parameters.

Administrator privileges needed

These software installation and set up tasks require the installer to have administration privileges for the particular user PC that is functioning as the client.

Single-user mode needed

These software installation and set up tasks assume that the administrator is in the single-user mode for the Windows® system. If the Windows® system is configured for the multiuser mode and multiple users log into the Windows® system simultaneously, unexpected problems can occur.

Keep patch levels current

The administrator must keep the patch level current for user PC clients that are running Windows® 2000, Windows® XP, Internet Explorer, and the DirectX® application programming interface in conjunction with the management system.

Important! The administrator must install all Microsoft® security patches issued for user PC clients that are running Microsoft® software in conjunction with the management system.

Microsoft® IE 7.0 Considerations

Microsoft® IE 6.0 and Microsoft® IE 7.0

The OMS GUI can run either Microsoft® IE 6.0 (IE6) or Microsoft® IE 7.0 (IE7). Users who want to upgrade to IE7 should note that certain browser configuration options must be made, the plug-in must be reconfigured, and certificate errors must be rectified before IE7 functions properly with the OMS GUI.

Microsoft® IE 7.0 broswer configuration

During installation of Microsoft® Internet Explorer 7.0 (IE7), the installation process may prompt the user for three different configuration options:

- *Pop-up Blocker Configuration*
  Because OMS displays many child screens, pop-up blocking should be turned off. After IE7 installation, this feature can be configured from the Tools menu bar.
- *Phishing Filter*
  The phishing filter feature examines websites against a known Microsoft® database for web sites that are known to collect personal information. The phishing filter should be disabled to improve performance of the OMS GUI. After IE7 installation, this feature can be configured from the Tools menu bar.
- *Add-On Management*
  Add-ons are plugin functions that extend the capability of the browser. When used with the OMS GUI, users can install IE7.0 with the following Add-ons:
  —Acrobat Reader (AcroIEHlprObj)
  —Diagnose Connection Problem
  —DriveLetter Access
  —Research
  —Send to Bluetooth Device
  —SVVHelper
  —Sun Java Console
  —Window Messengers

Java plug-in reconfiguration

When IE6 is upgraded to IE7 installation, users should run the OMS GUI auto configuration tool again to reconfigure the java plugin configuration properly. Rerunning the auto configuration tool should resolve any potential JRE plug-in failures that might occur after logging in to the OMS GUI. Refer to the "Run the Auto Configuration Tool for the Client Set Up" (p. 3-6) procedure for details.

Security Certificate Management

When users first the access the OMS GUI login screen, the IE7 browser intercepts the login page request and displays a certificate error screen, which is a warning to users that a problem exists with the encryption certificate. The certificate error screen is displayed for the following two reasons:

1. The name of the OMS computer is not the same as the URL hostname; a host mismatch has occurred.
2. The signing authority, Alcatel-Lucent, is not an officially recognized signing authority.

From the certificate error screen, users can choose the continue hyperlink to proceed on to the login screen or they can perform some simple certificate configurations to allow unfettered access to the OMS GUI login screen. The two configuration steps are the following:

1. Configure the IE7 browser to disable the host mismatch warning. Refer to the "Disable the Hostname Mismatch Warning for Microsoft® IE 7.0" (p. 3-37) for details.
2. Import the OMS encryption certificate into the trusted certificate authority list. Refer to the "Import the OMS Encryption Certificate for Microsoft® IE 7.0" (p. 3-38) task for details.

Related tasks

The following tasks are related to Microsoft® IE 7.0:

- "Configure Microsoft® IE 7.0" (p. 3-35)
- "Run the Auto Configuration Tool for the Client Set Up" (p. 3-6)
- "Disable the Hostname Mismatch Warning for Microsoft® IE 7.0" (p. 3-37)
- "Import the OMS Encryption Certificate for Microsoft® IE 7.0" (p. 3-38)

Run the Auto Configuration Tool for the Client Set Up

When to use

Use this task to run the Auto Configuration tool for the client set up.

You need administrator privileges on the client in order to run the AutoConfig.jsp tool.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Log in to OMS for the First Time" (p. 3-33)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2).

Task

Complete the following steps to run the Auto Configuration tool for the client set up.

1 Open the following page using your Internet Explorer:

http://<oms web server>/osm/jsp/core/AutoConfig.jsp

Example: http://summer.ho.lucent.com/osm/jsp/core/AutoConfig.jsp

2 When the Auto Configuration tool asks you to accept a digitally signed applet, accept it.

Result: The total procedure takes a few minutes. Once the page says the `PC configuration is completed`, go to "Log in to OMS for the First Time" (p. 3-33) task to log in.

END OF STEPS

Verify the Version of the Microsoft® Service Pack

When to use

Use this task to verify the version of the Microsoft® Service Pack (SP).

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to verify the version of the Microsoft® Service Pack.

1 At the PC client, navigate using the following path:

Start > Setting > Control Panel

2 Double click the **System** icon.

Result: The System Properties pop-up window is displayed showing the General tab.

3 On the General tab, verify the version of the Service Pack, which appears under the heading of **System:**

Result: For a Windows® 2000 PC, if the General tab does not display a Service Pack number or if the Service Pack is SP1, go to Step 4 to download the correct Service Pack. If the Service Pack is SP2, continue with the installation by going to the "Verify the Version and Text Size of Microsoft® IE 6" (p. 3-15) task or upgrade to SP3 by going to Step 4. We recommend that you upgrade to SP3.

For a Windows® XP Professional, the Service Pack must be SP1 or higher. OMS is certified to function properly on SP1 or higher.

4 For a Windows® 2000 PC, download SP3 by going to the following website:

http://www.microsoft.com/windows2000

5 Navigate using the following path:

Downloads > Service Packs

6 Select **Windows 2000 Service Pack 3** and follow the directions given.

7 Go to the "Verify and Set Virtual Memory Size" (p. 3-9) task to continue with the PC client set up.

END OF STEPS

Verify and Set Virtual Memory Size

When to use

Use this task to verify the size of virtual memory.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to verify the size of virtual memory.

1 At the PC client, navigate using the following path:

Start > Setting > Control Panel

2 Double click the **System** icon.

Result: The System Properties pop-up window is displayed.

3 Select the **Advanced** tab.

Result: The Advanced pop-up panel is displayed.

4 In the Advanced panel, click on **Performance Options** tab.

Result: The Performance Options pop-up panel is displayed.

5 In the Performance Options panel, verify that the following settings are correct; and if they are incorrect, correct them.

- In the **Applications response** section, the **Applications** radio button must be selected.
- In the **Virtual memory** section, the **Total paging file size for all drives** must be less than or equal to the physical memory size. (Example: When the physical memory size is 256MB, the total paging file size should be 128Mb or 256MB.)
  If it is not, click the **Change** button. The **Virtual Memory** pop-up panel is displayed. Increase the **Initial size** and **Maximum size** values.
  Set the **Recommended** size in **Total paging file size for all drives** to the initial size. Set the initial value multiplied by 2 to the maximum size. Click **Set** and then click **OK**.

6 Go to the "Disable Polling Sounds and Pop-Up Inhibiting Software" (p. 3-11) task to continue with the client set up.

END OF STEPS

Disable Polling Sounds and Pop-Up Inhibiting Software

When to use

Use this task to disable polling sounds and pop-up inhibiting software.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Have on-hand any vendor documentation when disabling pop-up inhibiting software.

Task

Complete the following steps to disable polling sounds and pop-up inhibiting software.

1 At the PC client, navigate using the following path:

Start > Setting > Control Panel

2 Double click the **Sounds and Multimedia** icon.

Result: The Sounds and Multimedia Properties pop-up window is displayed.

3 In the **Sounds Events** list, scroll down to **Windows Explorer**.

4 Select the **Start Navigation**.

5 Under the heading of **Name:**, use the drop down list to select **None**.

Result: The speaker icon in front of Windows Explorer disappears.

6 Click the **OK** button.

7 To disable any pop-up inhibiting software that might be installed on the PC client, refer to the appropriate vendor documentation and disable this software now.

8 Go to the “Set Font Size” (p. 3-13) task to continue with the PC client set up.

END OF STEPS

Set Font Size

When to use

Use this task to set the font size for the management system.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to set the font size for the management system.

1 At the PC client, navigate using the following path:

Start > Setting > Control Panel

2 Double click the **Display** icon.

Result: The Display Properties pop-up panel is displayed.

3 Select the **Settings** tab.

Result: The Settings panel is displayed.

4 Click the **Advanced** button.

Result: The (Multiple Monitors) and Mobility M3 Properties pop-up panel is displayed.

5 In the **Display** section, select **Small Fonts**, whose typical size is 96 dpi.

6 Click the **OK** button.

7 Go to the “Verify the Version and Text Size of Microsoft® IE 6” (p. 3-15) task to continue with the PC client set up.

END OF STEPS

Verify the Version and Text Size of Microsoft® IE 6

When to use

Use this task to verify the version and text size of Microsoft® Internet Explorer (IE).

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Verify the Version of the Microsoft® Service Pack" (p. 3-7)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to verify the version and text size of Microsoft® IE.

1 Open an instance of Microsoft® IE.

2 From the Microsoft® IE top menu bar, navigate using this path to verify the browser version:

Help > About Internet Explorer

Result: The About Internet Explorer pop-up window is displayed.

3 Verify the version Microsoft® IE, which appears as the first line of text.

Result: The Microsoft® IE version must be Version 6.

4 Click the **OK** button to close the About Internet Explorer pop-up window.

Result: The About Internet Explorer pop-up window closes.

5 From the Microsoft® IE top menu bar, navigate using this path to verify the text size:

View > Text Size

Result: A pop-up window showing various text sizes is displayed.

6 Verify that the Text Size is set to **Medium**.

Result: If the Text Size is set to Medium, go to Step 8.

If the Text Size is not set to Medium, the management system screens will be truncated. To set the Text Size to Medium, go to Step 7.

7 If the Text Size is not set to Medium, click on **Medium**.

Result: The Text Size is changed to Medium.

8 If your browser uses a proxy server to access the public internet, go to the "Configure the Proxy Server for Microsoft® IE" (p. 3-17) task to continue with the PC client set up.

If your browser does not use a proxy server to access the public internet, go to the "Configure the Browser Environment for Microsoft® IE" (p. 3-19) task to continue with the PC client set up.

END OF STEPS

Configure the Proxy Server for Microsoft® IE

When to use

If your browser uses a proxy server to access the public internet, use this task to configure the proxy server for Microsoft® Internet Explorer (IE).

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

The management assumes that a cache device does not exist between the PC clients running the management system and the web server. If your web browser has to use a proxy server (because of company policy or your personal network configuration) the proxy server should be configured so it does not cache html files; not caching html files ensures that the management system works properly.

Task

Complete the following steps to configure the proxy server for Microsoft® IE.

1 Open an instance of Microsoft® IE.

Result: The browser is displayed on your desktop.

2 From the top menu bar of Microsoft® IE, navigate to this path:

Tools > Internet Options

Result: The Internet Options pop-up window is displayed.

3 Click the **Connections** tab.

Result: The Connections panel is displayed.

4 Click the **Lan Settings...** button.

Result: The Local Area Network (LAN) Settings pop-up window is displayed.

5 Check the **Bypass proxy server for local addresses** box.

6 Click the **Advanced** button.

Result: The Proxy Server pop-up window is displayed.

7 Type the domain name of your web site into the text area at the bottom. Use semicolons to separate entries. Domain levels should be two or three levels.

Example: **ho.lucent.com** or **lucent.com**

8 Go to the "Configure the Browser Environment for Microsoft® IE" (p. 3-19) task to continue with the PC client set up.

END OF STEPS

Configure the Browser Environment for Microsoft® IE

When to use

Use this task to configure the web browser environment for Microsoft® Internet Explorer (IE).

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to configure the web browser environment for Microsoft® IE.

1 Open an instance of Microsoft® IE.

Result: The browser is displayed on your desktop.

2 From the top menu bar of Microsoft® IE, navigate to this path:

Tools > Internet Options

Result: The Internet Options pop-up window is displayed.

3 Click the **Advanced** tab.

Result: The Advanced panel is displayed.

4 Click the **Restore Defaults** button.

Result: All default settings are restored.

5 If you must customize any settings, only change those settings whose meaning you understand.

Important! The setting for **Disable script debugging**, which is the fourth item under **Browsing**, must be selected (the default) if you want to suppress the pop-up messages that Java™ script errors generate.

6 Click the **OK** button.

Result: All default settings are restored and any customized settings are saved.

7 Click the **Security** tab.

Result: The Security panel is displayed.

If the web page currently opened is located outside of the company network, that is, outside of the intranet network, the first icon **Internet** is automatically selected.

If the web page currently opened is located inside of the company network, that is, it is the intranet network, the second icon **Local Intranet** is selected. (If the web server for management system is located within your intranet network, as it should be, the second icon is selected.)

8 To ensure that all security settings are the defaults, click the **Default Level** unless the installation requires a customized security level.

9 To enable the **save** function in the table component, enable all the ActiveX controls under **Custom Level** and click the **Custom Level** button.

10 Select **Enable** for all five options under ActiveX controls and plug-ins.

Note: Enabling all five ActiveX options might introduce a security hole if the browser is used for other public web sites.

11 If you must further customize the security settings, you should fully understand the meaning and impact of what you are changing. Otherwise, do not change the default configuration except for enabling the ActiveX controls.

Important! If you change any security settings, you must enable the **Allow per-session cookies (not stored)**. If you fail to enable the **Allow per-session cookies (not stored)** setting, a problem can occur when using the management system. However, the management system does not require you to enable the permanent cookie, which is **Allow cookies that are stored on your computer**.

12 Click the **OK** button.

13 If the PC client you are setting up is running Windows® 2000, go to the "Verify the Version of the DirectX® Application Programming Interface " (p. 3-22) task to continue with the PC client set up.

If the PC client you are setting up is running Windows® XP Professional, go to the "Verify the Version of the Java™ Plug-in" (p. 3-24) task to continue with the PC client set up.

END OF STEPS

Verify the Version of the DirectX® Application Programming Interface

When to use

Use this task to verify the version of Microsoft® DirectX® application programming interface if you are setting up a Windows® 2000 PC.

Important! If the PC client that you are setting up is a Windows® XP Professional PC, this task does not have to be completed because Windows® XP Professional is bundled with Microsoft® Version 8.1. Go to the "Verify the Version of the Java™ Plug-in" (p. 3-24) task to continue with the PC client set up.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to verify the version of the DirectX® application programming interface.

1 At the PC client, navigate using the following path:

Start > Run

Result: The Run dialog pop-up window is displayed.

2 In the **Open:** box of the Run dialog pop-up window, enter the following command to determine if the DirectX® application programming interface is installed and if it is installed, its version number:

dxdiag

3 Click the **OK** button.

Result: The DirectX® Diagnostic Tool dialog box is displayed, showing the first tab, which is **System**. The version number appears in the **System Information** section, in the **DirectX Version** field.

4 Verify that the version number of the DirectX® application programming interface is Version 8.1 or higher.

Result: If the version of the DirectX® application programming interface is Version 8.1 or higher, go to the "Verify the Version of the Java™ Plug-in" (p. 3-24) task to continue with the PC client set up.

If the version of the DirectX® application programming interface is not Version 8.1 or higher, go to Step 5.

5 If the DirectX® application programming interface is not version 8.1 or higher, download the Version 8.1 or higher by going to the following website and following the directions given:

http://www.microsoft.com/windows/directx/downloads/default.asp

6 Once the DirectX® application programming interface Version 8.1 or higher is downloaded and installed, reboot the PC client.

7 Go to the "Verify the Version of the Java™ Plug-in" (p. 3-24) task to continue with the PC client set up.

END OF STEPS

Verify the Version of the Java™ Plug-in

When to use

Use this task to verify the version of the Java™ Runtime Environment (Plug-in).

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Important! The Java™ Plug-in must be 1.6.0_02. If the Java™ Plug-in is a *earlier version*, such as 1.4.1.x or an earlier 1.4.2 version, it is essential that the earlier version plug-in is uninstalled before the 1.6.0_02 version is installed.

Task

Complete the following steps to check the version of the Java™ Plug-in.

1 At the PC client, navigate using this path to verify that a Java™ Plug-in is installed and its version:

Start > Settings > Control Panel

Result: The Control Panel is displayed.

2 Verify that a Java™ Plug-in is installed by looking for the Java-Plug-in icon, which is a cup of steaming coffee.

Note: Many times, the Java™ Plug-in icon displays the version number directly below the icon.

Result: If the Java™ Plug-in icon is displayed and it shows the correct version of 1.6.0_02, go to the "Set Up Java™ Plug-in Runtime Parameters" (p. 3-29) task to continue with the PC client set up.

If the Java™ Plug-in is displayed and it does not show the correct version of 1.6.0_02, the Java™ Plug-in that is currently installed must be uninstalled. Go to the "Uninstall an Existing Java™ Plug-in" (p. 3-26) task to continue with the PC client set up.

If the Java™ Plug-in icon is displayed and it does not show any version number, go to Step 3 to check the version number.

If the Java™ Plug-in icon is not displayed, go to "Install the Java™ Plug-in" (p. 3-28) to continue with the PC client set up.

3 Double click the Java™ Plug-in icon.

Result: The Java™ Plug-in Control Panel is displayed.

4 Select the **About** tab.

Result: The Java™ Plug-in Control Panel About tab displays the version number of the Java Plug-in. The Java™ Plug-in must be Version 1.6.0_02.

5 If the Java™ Plug-in is Version 1.6.0_02, the Java™ Plug-in that is currently installed is correct. Go to the "Set Up Java™ Plug-in Runtime Parameters" (p. 3-29) task.

If the Java™ Plug-in is not Version 1.6.0_02, the Java™ Plug-in that is currently installed must be uninstalled. Go to the "Uninstall an Existing Java™ Plug-in" (p. 3-26) task.

END OF STEPS

Uninstall an Existing Java™ Plug-in

When to use

Use this task to uninstall an existing version of the Java™ Runtime Environment (Plug-in).

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Verify the Version of the Java™ Plug-in" (p. 3-24)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Important! The Java™ Plug-in must be 1.6.0_02. If the Java™ Plug-in is a *earlier version*, such as 1.4.1.x or an earlier 1.4.2 version, it is essential that the earlier version plug-in is uninstalled before the 1.6.0_02 version is installed.

Task

Complete the following steps to uninstall an existing version of a Java™ Plug-in.

1 At the PC client, navigate using this path:

Start > Settings > Control Panel > Add/Remove Programs

Result: A pop-up window list is displayed.

2 Select the **Java™ Runtime Environment** that is the incorrect version, which is the version other than version 1.6.0_02.

3 Click the **Change/Remove** button.

Result: If the program asks about shared files, go to Step 4.

If the program does not ask about shared files, go to Step 5.

4 If the program asks about shared files, select **No to all**.

5 After the uninstallation task is completed, right click anywhere in the Control Panel to bring up the pop-up menu and select **Refresh.**

Result: If the uninstallation is successful, the icon for the Java™ Plug-in disappears after the Refresh.

6 Repeat this task until all Java™ Plug-ins are uninstalled.

7 Go to the "Install the Java™ Plug-in" (p. 3-28) task to continue with the PC client set up.

END OF STEPS

Install the Java™ Plug-in

When to use

Use this task to install the **1.6.0_02** version of the Java™ Runtime Environment (Plug-in).

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

You need administrator privileges on the PC in order to install the Java plug-in.

Task

Complete the following steps to install the 1.6.0_02 version of a Java™ Plug-in.

1 Open an instance of Microsoft® Internet Explorer.

Result: The browser is displayed on your desktop.

2 Navigate to the OMS website by specifying the following:

http://<web server name>.hr.lucent.com.

Result: A web page is displayed that shows a hyperlink to the Plug-in.

3 Click on the hyperlink for the 1.6.0_02 Plug-in version.

Result: The Java™ Plug-in installation wizard is displayed.

4 Follow the prompting sequence of the Java™ Plug-in installation wizard by clicking **Yes** or **OK**.

5 After the installation task is completed, go to the "Set Up Java™ Plug-in Runtime Parameters" (p. 3-29) task to set up the correct runtime parameters.

END OF STEPS

Set Up Java™ Plug-in Runtime Parameters

When to use

Use this task to set up the Java™ Plug-in runtime parameters.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to set up the Java™ Plug-in runtime parameters.

1 At the PC client, navigate to this path to set up Java™ Plug-in runtime parameters:

Start > Settings > Control Panel

Result: The Control Panel is displayed.

2 Double click the Java™ Plug-in 1.6.0_02 icon.

Result: The Java™ Plug-in Control Panel is displayed.

3 Select the **Basic** tab.

Result: The Java™ Plug-in Control Panel Basic panel is displayed.

4 In the Basic panel, verify that the following settings are correct; and if they are incorrect, correct them.

Enable Java Plug-in must be checked.

Do not start console radio button must be selected.

Important! If you select **Hide console**, Microsoft® IE can randomly freeze.

Show Exceptions Dialog box must not be checked.

For the settings to take effect, click **Apply** or **Reset**.

5 Select the **Advanced** tab.

Result: The Java™ Plug-in Control Panel Advanced panel is displayed.

6 In the **Java Runtime Parameters** parameters field, you must set the initial and maximum memory sizes and other parameters to avoid Microsoft® IE freeze problems.

For a PC with 256MB or up to 512MB of memory, type the following parameters into the **Java Runtime Parameters** text field:

```
-Xms64m -Xmx256m -Dsun.java2d.noddraw=true
```

For the settings to take effect, click **Apply** or **Reset**.

Result: The Java™ Plug-in memory is allocated 64MB as its initial size and its memory allocation can increase to 256MB as its maximum size.

Note: Depending on the hardware specification, different memory allocations can be specified.

END OF STEPS

Clear the Java™ Plug-in Cache

When to use

Use this task to clear the Java™ Plug-in cache if the management system GUI picks up an old cached version of the Java™ Plug-in **.jar** file.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

This task can be completed in one of two methods. Method one clears the **cache** directory; method 2 deletes the **cache** directory.

Task: Method 1

Complete the following steps to clear the Java™ Plug-in cache.

1 At the PC client, navigate to this path to set up Java™ Plug-in runtime parameters:

Start > Settings > Control Panel

Result: The Control Panel is displayed.

2 Double click the Java™ Plug-in 1.6.0_02 icon.

Result: The Java™ Plug-in Control Panel is displayed.

3 Select the **Cache** tab.

Result: The Java™ Plug-in Control Panel Cache panel is displayed.

4 Click the **Clear** button to clear the cache.

5 Select the **Yes** button to confirm the clear.

Result: The Java™ Plug-in cache is now cleared.

END OF STEPS

Task: Method 2

Complete the following steps to clear the Java™ Plug-in cache by deleting the **cache** directory.

1 On a Windows 2000 PC, navigate to this path to clear Java™ Plug-in cache:

c:\Documents and Settings\<user>\Application Data\Sun\Java\Deployment\cache

Result: You are in the **cache** directory

2 Double click on the **cache** directory.

3 Follow this navigation sequence:

File > Delete

Result: The cache directory is deleted.

END OF STEPS

Log in to OMS for the First Time

When to use

Use this task to log in to the OMS (the management system) for the first time as the administrator.

Related information

See the following topic in this document:

- "Important Information about the Client Set Up" (p. 3-2)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to log in to the management system for the first time.

1 Open an instance of Microsoft® Internet Explorer.

Result: The browser is displayed on your desktop.

2 Navigate to the OMS website by adhering to the following:

If the address of the server is:

http://<web server name>.hr.lucent.com

navigate to:

http://<web server name>.hr.lucent.com/osm/jsp/core/Login.jsp

Result: The OMS login page is displayed.

3 Log in to the management system using the following user ID and password:

User ID: adminusr

Password: adminusr

Result: The Security Alert pop-up window appears.

4 Read the questions that appear on the pop-up windows and select the appropriate responses to continue.

Result: You are logged into the Administrative subsection of the management system.

5 Check the PC settings that you just made.

If any settings are incorrect, repeat the particular task. Be aware that many tasks require previous tasks to be completed.

END OF STEPS

Configure Microsoft® IE 7.0

When to use

Use this task to configure Microsoft® IE 7.0 during the installation process.

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Microsoft® IE 7.0 Considerations" (p. 3-4)
- "Configure Microsoft® IE 7.0" (p. 3-35)
- "Run the Auto Configuration Tool for the Client Set Up" (p. 3-6)
- "Disable the Hostname Mismatch Warning for Microsoft® IE 7.0" (p. 3-37)
- "Import the OMS Encryption Certificate for Microsoft® IE 7.0" (p. 3-38)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to configure Microsoft® IE 7.0 during the installation process.

1 During installation of Microsoft® Internet Explorer 7.0 (IE7), the installation process prompts for three different configuration options. Select the following:

Pop-up Blocker should be turned off. After IE7 installation, this feature can be configured from the Tools menu bar.

*Phishing Filter*should be disabled. After IE7 installation, this feature can be configured from the Tools menu bar.

Add-On Management install IE7.0 with the following Add-ons:

—Acrobat Reader (AcroIEHlprObj)

—Diagnose Connection Problem

—DriveLetter Access

—Research

—Send to Bluetooth Device

—SVVHelper

—Sun Java Console

—Window Messengers

2 When IE6 is upgraded to IE7 installation, run the OMS GUI auto configuration tool again to reconfigure the Java plug-in configuration properly. Refer to the "Run the Auto Configuration Tool for the Client Set Up" (p. 3-6) procedure for details.

3 When you first access the OMS GUI login screen, the IE7 browser intercepts the login page request and displays a certificate error screen. From the certificate error screen, you can perform some simple certificate configurations to allow unfettered access to the OMS GUI login screen. Proceed to the "Disable the Hostname Mismatch Warning for Microsoft® IE 7.0" (p. 3-37) and "Import the OMS Encryption Certificate for Microsoft® IE 7.0" (p. 3-38) tasks to resolve this problem.

END OF STEPS

Disable the Hostname Mismatch Warning for Microsoft® IE 7.0

When to use

Use this task to disable the hostname mismatch warning for Microsoft® IE 7.0.

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Microsoft® IE 7.0 Considerations" (p. 3-4)
- "Configure Microsoft® IE 7.0" (p. 3-35)
- "Import the OMS Encryption Certificate for Microsoft® IE 7.0" (p. 3-38)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

Task

Complete the following steps to disable the hostname mismatch warning for Microsoft® IE 7.0.

1 Open an instance of Microsoft® IE 7.0.

Result: The browser is displayed on your desktop.

2 From the Tools pop-up menu, select **Internet Options**.

Result: The Internet options pop-up window is displayed.

3 Select the **Advanced** tab on the Internet Options pop-up window.

Result: The Advanced settings panel is displayed.

4 Unselect the **Warn about certificate address mismatch*** checkbox.

5 Press the **OK** button on the bottom of the panel to save the configuration

END OF STEPS

Import the OMS Encryption Certificate for Microsoft® IE 7.0

When to use

Use this task to import the OMS Encryption Certificate for Microsoft® IE 7.0 for each OMS host that is to be accessed.

Related information

See the following topics in this document:

- "Important Information about the Client Set Up" (p. 3-2)
- "Microsoft® IE 7.0 Considerations" (p. 3-4)
- "Configure Microsoft® IE 7.0" (p. 3-35)
- "Log in to OMS for the First Time" (p. 3-33)
- "Run the Auto Configuration Tool for the Client Set Up" (p. 3-6)
- "Disable the Hostname Mismatch Warning for Microsoft® IE 7.0" (p. 3-37)

Before you begin

Read "Important Information about the Client Set Up" (p. 3-2) because these installation tasks must be completed in a certain order.

You must repeat this procedure for each OMS host that is to be accessed.

Task

Complete the following steps to import the OMS Encryption Certificate for Microsoft® IE 7.0.

1. Complete the first three steps in the "Log in to OMS for the First Time" (p. 3-33) task.

2. On the certificate warning screen, click the hyperlink to continue on to the OMS login page.

   Result: The OMS login page is displayed.

3. Click on the red shield in the red **Certificate Error** box.

   Result: A pop-up dialog, which is also titled Certificate Error, is displayed.

4. Select the **View Certificate** hyperlink at the bottom of the pop-up dialog.

Result: The pop-up dialog is closed. Detailed information about the certificate is displayed in a the **Certificate** pop-up window.

5 Click the **Install Certificate...** button on the bottom of the Certificate pop-up window.

Result: The Certificate Import Wizard pop-up is displayed.

6 Click the **Next** button on the first page of the Certificate Import Wizard pop-up.

7 On the second page of the Certificate Import Wizard, select the **Automatically select the certificate store based on the type of certificate** button.

8 Click the **Next** button to display the final wizard screen.

9 Click the **Finish** button on the final wizard screen.

Result: A Security Warning dialog box is displayed that asks you to acknowledge the import operation and to install the certificate.

10 Click the **Yes** button on the dialog box to accept the import operation and to install the certificate.

11 Click **OK** to close the success operation dialog.

12 Click **OK** on the Certificate screen to close the screen.

Result: Once the OMS encryption certificate is imported and the hostname mismatch warning is disabled, subsequent access of the OMS login screen are no longer routed to the IE7 certificate warning screen. Note that the certificate for each OMS host needs to be imported separately. In other words, you must repeat this procedure for each OMS host that is to be accessed.

END OF STEPS

4 Cut Throughs

Overview

Purpose

This chapter explains how to configure the OMS PC client to enable cut-through capabilities from the OMS to other remote sites, such as element management systems or craft interface terminals (CITs).

Contents

Cut Through Concepts

Cut-throughs to supported remote sites

OMS supports cut-through capabilities from the OMS PC client to a *remote site*, which includes GUI clients of other element management systems and/or the craft interface terminals (CITs) of NEs.

The management system supports cut-through capabilities from the OMS PC client to the following remote sites:

- Navis® EMS (SNMS), providing certain PC hardware specifications are met on the OMS client. Refer to "Client hardware platform" (p. 2-3) for details.
- ITM-SC, providing certain PC hardware specifications are met on the OMS client. Refer to "Client hardware platform" (p. 2-3) for details.
- NAVIS® EMS-CBGX system and all CBX-3500 switches that NAVIS® EMS-CBGX manages
- 1675 Lambda Unite MultiService Switch (MSS) craft interface terminal (CIT)
- 1625 LambdaXtreme® Transport craft interface terminal (CIT)
- Network Management Adapter (NMA) to provision 1671 Service Connect (SC) ports. Refer to "Cut-Through from OMS GUI to NMA GUI for Port Provisioning" (p. 4-31) for details.

Cut-through supported platforms

The use of cut-through capabilities from the OMS PC client to the particular remote site is supported on the *Server Platforms*.

Backward compatibility and the default location of the remote site software

For all instances, the remote site software is backward compatible to its previous releases. We recommend that users always install the latest version of the software and delete previous versions for space saving considerations.

Once installed, the remote site software can be found in the following default directories:

- For the NAVIS® EMS-CBGX system:
  C:\Lucent\NavisEMS-CBGX\Client
- For the 1675 Lambda Unite MultiService Switch (MSS) CIT:
  C:\Program Files\Lucent Technologies\WaveStar CIT
- For the 1625 LambdaXtreme® Transport CIT:
  C:\Program Files\Alcatel-Lucent\LX_Xport CIT

Under certain circumstances, such as insufficient disk space or for archival purposes prior to an upgrade, users can install and/or move the remote site software to another location on the same disk or to an external disk and still be able to launch the particular CIT or GUI client from that default location. Refer to "Launch the Remote Site Software Away from the Default Location" (p. 4-22) task for details.

The java.policy file for the cut-throughs

The property, file, and socket permissions in the **java.policy** file must be set so the OMS management system can access system files. Refer to the "Configure the java.policy File for Cut-Through" (p. 4-25) task for detailed instructions.

Once the **java.policy** file is modified, the browser must be closed and reopened for any changes to take effect. The management system can then access the command files that are needed to invoke the cut-through to the remote site software. These command files are explained in detail in "Command Files for the Cut-Through" (p. 4-4) section and in the "Customize the Command Files for Cut-Through" (p. 4-30) task.

Order of task execution for cut-through

To support the display of the remote site software (EMS GUI client or NE CIT) from the pages of the OMS management system, execute the following tasks in the order in which they follow:

1. Execute the "Verify the OMS Client Hardware Configuration" (p. 4-9) task.
2. Execute the appropriate installation and/or configuration task:
   Install the Navis® EMS (SNMS) GUI. Refer to the appropriate Navis® EMS (SNMS) installation documentation for details.
   Execute the "Configure ITM-SC" (p. 4-11) task.
   "Install the NAVIS® EMS-CBGX System" (p. 4-16) task
   "Install the 1675 Lambda Unite MultiService Switch (MSS) CIT" (p. 4-18) task
   "Install the 1625 LambdaXtreme® Transport CIT" (p. 4-20) task
3. If needed, execute the "Launch the Remote Site Software Away from the Default Location" (p. 4-22) task.
4. Execute the "Configure the java.policy File for Cut-Through" (p. 4-25) task.
5. If needed, execute the "Customize the Command Files for Cut-Through" (p. 4-30) task.

Time synchronization with NTP

When the date/time on the remote site and OMS platforms are not properly synchronized, the generation of correct PM reports for the indirectly managed NEs, which are those NEs that are managed through the remote site is not possible.

The OMS date/time synchronization feature supports directly managed NEs only. Indirectly managed NEs are typically synchronized through a procedure that is initiated from the CIT and/or GUI of the remote site.

Once a cut-through to the remote site CIT and/or GUI has been established, users can use Network Time Protocol (NTP) to synchronize the platform. NTP is widely used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem.

Command Files for the Cut-Through

The command files

Once the **java.policy** file has been modified so the management system can access system files, the management system PC client then uses the following files to invoke the cut-through to the remote site:

- The “cutthru.txt file” (p. 4-4) for all cut-throughs.
- The “cutthru.bat file” (p. 4-6) for all cut-throughs.
- A “Launch file” (p. 4-6) for the 1675 Lambda Unite MultiService Switch (MSS) CIT and the 1625 LambdaXtreme® Transport CIT.
- An “Executable file” (p. 4-7) for the Navis EMS-CBGX GUI client and supported CBX-3500 switches.

cutthru.txt file

The **cutthru.txt** file, which is a text file that the cut-through software uses, contains user-defined configuration parameters such as the following:

- enable debugging
- the directory location(s) of software to which the management system is to cut-through
- important mapping information
- the IP address of the local PC

The **cutthru.txt** file is commented with a detailed description of each parameter. Users should customize values in this file once so the management system can properly launch the particular cut-through.

The path to this file is as follows:

C:\cutthru.txt

Navis® EMS (SNMS) GUI:

For users who are trying to launch an Navis® EMS (SNMS) GUI, the release number and directory mappings must be properly defined in this file.

ITM-SC GUIs:

For users who are trying to launch an ITM-SC GUI, the **localHostIpAddress** variable must be configured. If the ITM-SC GUI does not run on the same host as the ITM_SC server, then the ITM-SC host to ITM-SC GUI server configuration must also be configured.

Refer to the "Customize the Command Files for Cut-Through" (p. 4-30) task for editing details.

Navis EMS-CBGX GUI client and supported CBX-3500 switches:

If the remote site is to be launched from its default directory for the cut-through to the Navis EMS-CBGX GUI client and supported CBX-3500 switches, the **cutthru.txt** file is not-relevant and does not have to be used or edited.

If the remote site is to be launched from another directory, the following parameters must be specified in the **cutthru.txt** file to indicate the path to the NavisEMS-CBGX GUI client software:

- **CBGXDRIVE**
- **CBGXROOT**

Refer to the "Customize the Command Files for Cut-Through" (p. 4-30) task for details.

1675 Lambda Unite MultiService Switch (MSS) and the 1625 LambdaXtreme® Transport CITs:

If the remote site is to be launched from its default directory for the 1675 Lambda Unite MultiService Switch (MSS) and the 1625 LambdaXtreme® Transport CITs, the associated TNA is co-resident with the OMS server, and the OMS GUI is invoked from the same OMS server, then the **cutthru.txt** file is irrelevant and does not have to be edited.

If the remote site is to be launched from another directory, the following parameters must be specified in the **cutthru.txt** file:

- **CITDRIVE**
- **CITROOT**

If any associated TNA is distributed from another server or if the OMS GUI is distributed from another server (even if the TNA is co-resident), one of the following parameters must be specified (one for each TNA involved) in the **cutthru.txt** file:

- **NAIP**
- **NAHOST**

Refer to the "Customize the Command Files for Cut-Through" (p. 4-30) task for details.

cutthru.bat file

The **cutthru.bat** is a batch file that OMS automatically generates to incorporate execution from the launching directory for the particular remote site. Users do not have to alter the content of this file. However, when the remote software is moved to a new location, users must delete this file so the new file that reflects the new location can be automatically regenerated.

The path and the names of the particular cutthru.bat files for the supported NEs are as follows:

- **C:\cutthruSNMS.bat** is the path and filename for the cutthru.bat file for the Navis® EMS (SNMS) GUI software.
- **C:\cutthruSC.bat** is the path and filename for the cutthru.bat file for ITM-SC GUI software.
- **C:\cutthruCBGX.bat** is the path and filename for the cutthru.bat file for Navis EMS-CBGX GUI client and supported CBX-3500 switches.
- **C:\cutthru_UNIE_CIT.bat** is the path and filename for the cutthru.bat file for 1675 Lambda Unite MultiService Switch (MSS).
- **C:\cutthru_LX_CIT.bat** is the path and filename for the cutthru.bat file for 1625 LambdaXtreme® Transport.
- **C:\cutthruEMA.bat** is the path and filename for the cutthru.bat file for 1671 Service Connect (SC) NEs.

Refer to the "Customize the Command Files for Cut-Through" (p. 4-30) task for details.

Launch file

For the 1675 Lambda Unite MultiService Switch (MSS) and 1625 LambdaXtreme® Transport NEs, the launch file is a text file that is used to invoke the CIT to pass parameters that are needed to communicate with the target NE. The two launch files are the following:

- **LaunchUniteGUI.bat** is the launch file for 1675 Lambda Unite MultiService Switch (MSS).
- **OMS-LaunchXtremeGUI.bat** is the launch file for 1625 LambdaXtreme® Transport.

If the CIT software does not contain this file, it can be obtained from the OMS host at the following URL:

https://<OMS host IP address>/CITDATA

Both the **LaunchUniteGUI.bat** and the **OMS-LaunchXtremeGUI.bat** files must be put at the root directory of the CIT software. If the CIT software is moved to another location, this file must also be moved.

Refer to the "Customize the Command Files for Cut-Through" (p. 4-30) task for details.

For 1671 Service Connect (SC) NEs, the launch file **C:\launchEMA.bat** is a text file that is used to invoke the NMA GUI to pass parameters that are needed to communicate with the target NMA server.

The **C:\launchEMA.bat** file is automatically populated at **C:\ALU\OMS_EMA\script** when the Network Management Adapter (NMA) GUI is installed in your PC.

Executable file

For the Navis EMS-CBGX GUI client and supported CBX-3500 switches, an executable file (an **.exe** file) is used to invoke the NavisEMS-CBGX GUI client, which is already configured to communicate with a particular NavisEMS-CBGX server. This file is populated to a subdirectory **bin** under the installation root directory, which is as follows:

C:\Lucent\NavisEMS-CBGX\Client\bin\NavisEMS-CBGXClient.exe

ITM-SC Concepts

ITM-SC login

The ITM-SC application uses UNIX® logins as the security mechanism for the ITM-SC GUI.

Users can have one of the following types of accounts:

- individual accounts
- share a single account (such as the administrator account *i2kadmin*)

Refer to the ITM-SC documentation for administration of login accounts for the ITM-SC GUI.

ITM-SC .rhosts file

During a management system cut-through request to launch the ITM-SC GUI, the management system GUI session uses a remote script to launch the ITM-SC GUI on the UNIX® machine that is running the ITM-SC GUI process. To allow the remote script to execute, the .**rhosts** file for the UNIX® login account must be configured to allow the PC that is running the management system GUI session to execute the remote script.

The **.rhosts** file must exist in the $HOME directory of the user account that is to run the ITM-SC GUI. The .**rhosts** file is a simple ASCII file that can contain the PC name or the remote PC username that is allowed to launch an ITM-SC GUI process. Each line of the file contains a separate user entry in the form:

```
{hostname} {optional username}
```

Example:

If a PC called *bombay* needs to invoke an ITM-SC session for the user account *i2kadmin*, the **.rhosts** file for user *i2kadmin* **(/home/i2kadmin/.rhosts)** would contain a single line entry as:

```
bombay
```

Note that each PC defined in the **.rhosts** file needs to be defined in the local name server or the **/etc/hosts** file that resides on the UNIX® machine.

To allow a user named *john* to launch the ITM-SC GUI, the **.rhosts** file for user *i2kadmin* **(/home/i2kadmin/.rhosts)** would contain a single line entry as:

```
+ john
```

Here, the plus symbol acts as a wild card for the hostname. The user name can be retrieved from the MS-DOS variable called *USERNAME*. (Use the **set** command to retrieve all MS-DOS variables.)

ITM-SC and the X-Windows Server

To support a management system cut-through to ITM-SC, an X-Window server must be installed on the PC.

The management system supports the X-Window server of Hummingbird's Exceed software. The default Exceed software installation, is sufficient for running the ITM-SC GUI on the PC.

Once the X-Window Server is installed, you must enable the ITM-SC GUI to display the management system GUI on the PC. See the “Configure ITM-SC” (p. 4-11) task for details.

Verify the OMS Client Hardware Configuration

When to use

Use this task to verify the hardware configuration of the OMS client.

Related information

See the following topic in this document:

- "Client hardware platform" (p. 2-3)
- "Cut Through Concepts" (p. 4-2)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

The recommended OMS client hardware configuration is detailed in "Client hardware platform" (p. 2-3). Use the information in this table to verify the hardware configuration of your OMS client.

This tasks has two methods. Choose either of the two methods.

Task: Method 1

Complete the following steps to verify the hardware configuration of the OMS client.

1 At your PC, which is the OMS client, navigate using the following path:

Programs > Accessories > System Tools > System Information

Result: The System Information pop-up window is displayed.

2 Verify the hardware information that is displayed at the bottom of the list to determine if your PC has the recommended amount of memory to run the management system.

END OF STEPS

Task: Method 2

Complete the following steps to verify the hardware configuration of the OMS client.

1 At your PC, which is the OMS client, right click on the **My Computer** icon and select **Properties**

Result: The **System Properties** window is displayed showing information in the **General** tab.

2 Verify the your PC has the recommended amount of RAM to run the management system.

3 Click on **Support Information**.

Result: A pop-up window bearing the PC manufacturer is displayed.

4 Scroll down the list and verify the applications that have been installed on your PC and, further down the list, verify the overall amount of memory that the machine has to run the management system.

END OF STEPS

Configure ITM-SC

When to use

Use this task to configure ITM-SC.

Related information

See the following topic in this document:

- "Cut Through Concepts" (p. 4-2)
- "ITM-SC Concepts" (p. 4-7)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

ITM-SC is configured to run as one of the following:

- as a single UNIX® computer running both the ITM-SC application and ITM-SC GUI user processes
- two (or more) UNIX® computers with one server running the ITM-SC application and the other computer(s) running the ITM-SC GUI user processes.
  If the ITM-SC server is running in this type of multi-box configuration, you must know the name of the server that runs the ITM-SC GUI for the management system cut-through.

Task

Complete the following steps to configure ITM-SC.

1 Create ITM-SC account so you can log in to ITM-SC. Refer to "ITM-SC login" (p. 4-7) for details.

Result: The directory is changed.

2 Edit the **.rhosts** file. Refer to "ITM-SC .rhosts file" (p. 4-7) for details.

3 Install the X-Windows Server on your PC. Refer to "ITM-SC and the X-Windows Server" (p. 4-8) for details.

4 Once the X-Windows installed, access Exceed's configuration utilities and in the **Host Access Control List** panel of the Security screen, select the **disabled** option.

END OF STEPS

Test the Cut-Through to the EMS and Synchronize Time

When to use

Use this task to test the cut-though that you have created to the EMS GUI and to synchronize time among ITM-SC, EMS, and OMS.

Related information

See the following topics in this document:

- "Cut Through Concepts" (p. 4-2)
- "Command Files for the Cut-Through" (p. 4-4)
- "ITM-SC Concepts" (p. 4-7)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

This task encompasses two parts:

- Part 1 of this task explains the steps needed to test the cut-though that you have created to the EMS GUI.
  Part 1 of this task can be done in one of two ways, which are documented here as Method 1 and Method 2. Each method requires a user role profile other than that of the NOC Administrator because you will have to access the Network Elements icon or the Network Map from the management system; therefore, Step 1 of each method requires you to log in to the management system and use or create a user role profile that enables NOC Expert Operator user tasks.
- Part 2 of this task explains the step needed to synchronize time among ITM-SC, EMS, and OMS. For more details on time synchronization, refer to "Time synchronization with NTP" (p. 4-3).

Part 1: Method 1

Complete the following steps to test the cut-through to the EMS via the Network Elements page.

1 Log in to the management system and use or create a user role profile that enables NOC Expert Operator user tasks. Use the "Add a User-Defined User Role Profile" (p. 7-25) if you have to customize a user role profile.

2 Navigate to the **Network Elements** page.

3 Select a subtending EMS NE.

4 From the **Go** menu, select **Open EMS/SC GUI**.

5 Click on **Go**.

Result: If the cut-through is successful, the EMS GUI is displayed.

END OF STEPS

Part 1: Method 2

Complete the following steps to test the cut-through to the EMS via the Network Map.

1 Log in to the management system and use or create a user role profile that enables NOC Expert Operator user tasks. Use the "Add a User-Defined User Role Profile" (p. 7-25) if you have to customize a user role profile.

2 Navigate to the Network Map.

3 Expand the areas to find a subtending EMS NE.

4 Select a subtending EMS NE.

5 From **Session**, select **Open EMS/SC GUI**.

6 Click on **Go**.

Result: If the cut-through is successful, the EMS GUI is displayed.

END OF STEPS

Part 2

Complete the following step to synchronize time:

1 To keep the EMS, ITM-SC, and OMS management platforms synchronized, synchronize each platform to the same Network Time Protocol (NTP) source. Refer to "Time synchronization with NTP" (p. 4-3) for details.

END OF STEPS

Install the NAVIS® EMS-CBGX System

When to use

Along with the appropriate NAVIS® EMS-CBGX documentation, use this task to install the NAVISEMS-CBGX system.

Related information

See the following topics in this document:

- "Cut Through Concepts" (p. 4-2)
- "CBGX-EMS User Name" (p. 6-36) installation parameter
- "CBGX-EMS Password" (p. 6-37) installation parameter
- "OMS_NE license" (p. 5-10) (OMS_NE_CBG)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

You cannot successfully complete this task unless you have the following:

- The NAVIS® EMS-CBGX documentation that fully explains how to install the GUI client
- The media on which the GUI client software is installed

Important! If the IP address of the NavisEMS-CBGS server is changed after the installation, or if you want your CBGX GUI client to communicate with another NavisEMS-CBGX server, you can re-configure the IP address and port numbers in either of the following two ways:

1. Repeat this entire installation procedure.
   Select **Install** in Step 2.
   Re-enter the new NAVISEMS_CBGX Server IP address and two port numbers in Step 3.
2. At runtime, when the software is launched, re-enter the new IP address and port numbers on the login pop-up.

Task

Complete the following steps to install the NAVIS® EMS-CBGX system.

1 Obtain the **install_NAVISEMS_CBGX_Client_{xx.yy.zz}.exe** and click on the filename to start the installation.

The default directory for the NAVIS® EMS-CBGX system is the following:

C:\Lucent\NavisEMS-CBGX\Client

2 When the installation program prompts you for **Upgrade** or **Install**, select **Install** for the first time installation.

Note: select **Upgrade** to un-install the existing version and to install a new version.

3 Enter the NAVISEMS_CBGX Server IP address and two port numbers.

Result: When the software is launched, communication is then established between the CBGX Client on your OMS PC client and the CBGX server at that IP address.

4 Enter the utility server IP address and the port number.

5 Wait a few minutes until the installation program displays an indication that it has completed.

END OF STEPS

Install the 1675 Lambda Unite MultiService Switch (MSS) CIT

When to use

Along with the NE CIT documentation, use this task to install the 1675 Lambda Unite MultiService Switch (MSS) craft interface terminal (CIT).

Related information

See the following topic in this document:

- "Cut Through Concepts" (p. 4-2)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

You cannot successfully complete this task unless you have the following:

- The 1675 Lambda Unite MultiService Switch (MSS) CIT documentation that fully explains how to install the CIT
- The media on which the CIT software is installed

Task

Complete the following steps to install the NE CIT.

1 Insert the CD-ROM.

The default directory for the 1675 Lambda Unite MultiService Switch (MSS) CIT is the following:

C:\Program Files\Lucent Technologies\WaveStar CIT

2 Select the **setup.exe** file by clicking or double clicking.

Result: The **setup.exe** file prompts you to complete the installation.

3 When **setup.exe** prompts you to complete the installation, make the following selections:

Choose to Disable the login/password.

Choose to install the client software at the default directory, which can easily be done by clicking on the prescribed path.

Choose not to connect the server via OSI.

Result: If the CIT software has installed successfully, you are done with this task.

If the CIT software has not installed successfully, go to Step 4.

4 If the CIT software does not contain the launch file (**LaunchUniteGUI.bat**), go to the following link to get the launch file:

https://<your OMS host IP address>/CITDATA

END OF STEPS

Install the 1625 LambdaXtreme® Transport CIT

When to use

Along with the NE CIT documentation, use this task to install the 1625 LambdaXtreme® Transport craft interface terminal (CIT).

Related information

See the following topic in this document:

- "Cut Through Concepts" (p. 4-2)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

You cannot successfully complete this task unless you have the following:

- The 1625 LambdaXtreme® Transport CIT documentation that fully explains how to install the CIT
- The media on which the CIT software is installed

Task

Complete the following steps to install the 1625 LambdaXtreme® Transport CIT.

1 Insert the CD-ROM.

The default directory for the 1675 Lambda Unite MultiService Switch (MSS) CIT is the following:

C:\Program Files\Alcatel-Lucent\LX_Xport CIT

2 Select the **setup.exe** file by clicking or double clicking.

Result: The **setup.exe** file prompts you to complete the installation.

3 When **setup.exe** prompts you to complete the installation, make the following selections:

Choose to install the client software at the default directory, which means you are to overwrite the pre-typed pathname to the following:

C:\Program Files\Alcatel-Lucent\LX_Xport CIT

Choose not to connect the server via OSI.

Result: If the CIT software has installed successfully, you are done with this task.

If the CIT software has not installed successfully, go to Step 4.

4 If the CIT software does not contain the launch file (**OMS-LaunchUniteGUI.bat**), go to the following link to get the launch file:

https://<your OMS host IP address>/CITDATA

END OF STEPS

Launch the Remote Site Software Away from the Default Location

When to use

Use this task to launch the remote site software (EMS GUI client or the NE CIT) away from its default location to another location.

Important! We recommend that the cut-through is installed in the default directory because it requires the minimal manual configuration. However, if you need to move the remote software to another location, or even to an external disk, you need to follow the steps in this task.

The remote software can be installed from the following locations:

- From a location other than the default location; see“Install the 1675 Lambda Unite MultiService Switch (MSS) CIT” (p. 4-18) or “Install the 1625 LambdaXtreme® Transport CIT” (p. 4-20) for details.
- On the default location, then moved to a new location.

The new root directory always includes a subdirectory (named **WaveStar CIT** or **LX_Xport CIT**) for the installation case, but may not for the move case.

Related information

See the following topic in this document:

- “Cut Through Concepts” (p. 4-2)

Before you begin

Follow the order of task execution that is specified in “Order of task execution for cut-through” (p. 4-3).

Task

Complete the following steps to launch the remote software (EMS GUI client or NE CIT) away from its default location to another location.

1 Move and/or install the remote software, which includes the 1675 Lambda Unite MultiService Switch (MSS) CIT, the 1625 LambdaXtreme® Transport CIT, or the Navis EMS-CBGX GUI client and supported CBX-3500 switches, to a non-default location.

2 In the **c:** directory, delete the **cutthru.bat** file for the particular NE if this file exists. (This file will be regenerated automatically once the NE CIT is moved to its new location.)

```
DE cutthru_UNITE_CIT.bat

DE cutthru_LX_CIT.bat

DE cutthruCBGX.bat
```

3 Edit the **C:cutthru.txt** file to specify the new location through the two variables below:

For the NE CITs:

- CITDRIVE {NE type} {new drive}
- CITROOT {NE type} {new root dir}\

For the Navis EMS-CBGX GUI client and supported CBX-3500 switches:

- CBGXDRIVE CBX {new drive}
- CBGXROOT CBX {new root dir}\

For the NE CITs:

If the file does not exist, create one. Note that the delimiter between words in brakets {} is one <\t>, which is one tab character.

Example 1: To install the CIT software to the **f** drive, directory **\Install Here**, the CIT can be launched from the following:

f:\Install Here\WaveStar CIT

Set:

```
CITDRIVE  UNITE f

CITROOT  UNITE \Install Here\WaveStar CIT\
```

Example 2: To move the CIT software to the **f** drive, directory **\Move Here**, the CIT can be launched from the following:

f:\Move Here

Set:

```
CITDRIVE  UNITE f

CITROOT  UNITE \Move Here\
```

Example 3: If the 1625 LambdaXtreme® Transport CIT software is installed in k:\NEW_XTREME_CIT, set:

```
CITDRIVE  LX k
```

```
CITROOT  LX \NEW_XTREME_CIT\LX_Xport CIT\
```

For the Navis EMS-CBGX GUI client and supported CBX-3500 switches, if the software is moved to **f:\myCBGX-GUI**:

```
CBGXDRIVE CBX f

CBGXROOT CBX \myCBGX-GUI\
```

4 For the 1675 Lambda Unite MultiService Switch (MSS) and 1625 LambdaXtreme® Transport CITs, if the CIT software does not contain the launch file (**LaunchUniteGUI.bat** or **OMS-LaunchXtremeGUI.bat**), go to the following link to get the launch file:

https://<your OMS host IP address>/CITDATA

5 Update the **java.policy** file to include the appropriate file permission. Refer to the "Configure the java.policy File for Cut-Through" (p. 4-25) task.

END OF STEPS

Configure the java.policy File for Cut-Through

When to use

Use this task to configure the **java.policy** file for a cut-through to a remote site, which includes cut-through to Navis® EMS (SNMS), ITM-SC, the NAVIS® EMS-CBGX system and all CBX-3500 switches that NAVIS® EMS-CBGX managesm, the 1675 Lambda Unite MultiService Switch (MSS) CIT, 1625 LambdaXtreme® Transport CIT and the NMA GUI for Port Provisioning.

Related information

See the following topic in this document:

- "Cut Through Concepts" (p. 4-2)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

The entries that you are to add to the **java.policy** file allow the management system GUI to create and run batch files to invoke EMS GUI clients or a subtending NE CIT.

Task

Complete the following steps to configure the **java.policy** file for a cut-through to a remote site, which includes cut-through to Navis® EMS (SNMS), ITM-SC, the NAVIS® EMS-CBGX system and all CBX-3500 switches that NAVIS® EMS-CBGX manages, the 1675 Lambda Unite MultiService Switch (MSS) CIT, and the 1625 LambdaXtreme® Transport CIT and the NMA GUI for Port Provisioning.

1 At your PC, navigate to this path to access the **java.policy** file.

C:\Program Files\Java\<java plug-in version>\lib\java.policy

Result: The directory is changed.

2 For the Navis® EMS (SNMS) GUI clients, go Step 3.

For the Navis EMS-CBGX GUI client and supported CBX-3500 switches, go Step 4.

For the 1675 Lambda Unite MultiService Switch (MSS) and 1625 LambdaXtreme® Transport CITs, go to Step 5.

For the 1671 Service Connect (SC) NMA GUI, go to Step 6

3 For the Navis® EMS (SNMS) GUI client, access the **java.policy** file using Wordpad or Notepad and add the following lines to the bottom of the file:

```
grant {

permission java.util.PropertyPermission "user.name", "read";

permission java.io.FilePermission "c:\\cutthru.txt", "read,write,
  execute";

permission java.io.FilePermission "c:\\cutthruSNMS.bat", "read,write,
  execute";

permission java.io.FilePermission "c:\\cutthruSC.bat", "read,write,
  execute";

permission java.lang.RuntimePermission "modifyThread";

permission java.lang.RuntimePermission "modifyThreadGroup";

permission java.net.SocketPermission "localhost:1024-","listen,
  resolve,accept";

permission java.lang.RuntimePermission "modifyThread";

permission java.lang.RuntimePermission "modifyThreadGroup";

};
```

Go to Step 7.

4 For the Navis EMS-CBGX GUI client and supported CBX-3500 switches, access the **java.policy** file using Wordpad or Notepad and add the following lines to the bottom of the file:

```
grant {

permission java.util.PropertyPermission "user.name", "read";

permission java.io.FilePermission "c:\\cutthru.txt","read,write,
  execute";

permission java.io.FilePermission "c:\\cutthruCBGX.bat","read,write,
  execute";

permission java.io.FilePermission "c:\\Lucent\\NavisEMS-CBGX
```

```
  \\Client\\bin\\NavisEMS-CBGXClient.exe",
  "read,write,execute";

permission java.lang.RuntimePermission "modifyThread";

permission java.lang.RuntimePermission "modifyThreadGroup";
  };
```

Go to Step 7.

5 For the 1675 Lambda Unite MultiService Switch (MSS) and 1625 LambdaXtreme® Transport CITs, access the **java.policy** file using Wordpad or Notepad and add the following lines to the bottom of the file:

```
grant {

permission java.util.PropertyPermission "user.name", "read";

permission java.io.FilePermission "c:\\cutthru.txt","read,write,
  execute";

permission java.io.FilePermission "c:\\cutthru_UNITE_CIT.bat","read,
  write,execute";

permission java.io.FilePermission "c:\\Program Files\\Lucent
  Technologies\\WaveStar CIT

  \\LaunchUniteGUI.bat","read,write,execute";

permission java.io.FilePermission "c:\\cutthru_LX_CIT.bat","read,
  write,execute";

permission java.io.FilePermission "c:\\Program Files\\Lucent
  Technologies\\LX_Xport CIT

  \\OMS-LaunchXtremeGUI.bat","read,write,execute";

permission java.net.SocketPermission "<TNA hostname>","resolve";

permission java.net.SocketPermission "<TNA hostname>:9099",
  "connect";

permission java.lang.RuntimePermission "modifyThread";

permission java.lang.RuntimePermission "modifyThreadGroup";

};
```

Important!

Note that the reserved port is 9099.

If the CIT software is moved away from the default directory, you must update this file to reflect the new disk drive and the path of the launching file (for example: **LaunchUniteGUI.bat** or **OMS-LaunchXtremeGUI.bat**).

If OMS manages NEs with multiple TNA servers, you must grant socket permission to each TNA server; meaning, you must repeat the two java.net.SocketPermission lines for each TNA server.

Go to Step 7.

6 For 1671 Service Connect (SC) NMA cut-through, access the **java.policy** file using Wordpad or Notepad and add the following lines to the bottom of the file:

```
//allows anyone to listen on un-privileged ports

permission java.net.SocketPermission "localhost:1024-", "listen,
  resolve,accept";

permission java.io.FilePermission "c:\\cutthru.txt", "read,write,
  execute";

permission java.io.FilePermission "c:\\cutthruEMA.bat", "read,write,
  execute";

permission java.io.FilePermission "c:\\ALU\\OMS_
  EMA\\script\\launchEMA.bat", "read,write,execute";

permission java.lang.RuntimePermission "modifyThread";

permission java.lang.RuntimePermission "modifyThreadGroup";
```

Important!

File *cutthru.txt* and file *cutthruEMA.bat* are automatically generated by the OMS GUI during execution; they are always located at **C:\**.

File *launchEMA.bat*, however, comes with the NMA GUI software package. It is populated to directory **C:\ALU\OMS_EMA\script\\** when the NMA GUI software is installed.

Go to Step 7.

7 Use the editor's **save** command to save the lines that you have just added.

Result: The changes made to the **java.policy** file are saved.

8 Close and reopen the browser so the changes that you have made to the **java.policy** file take effect.

Result: The changes have been made to the **java.policy** file have now taken effect.

END OF STEPS

Customize the Command Files for Cut-Through

When to use

Use this task to customize (edit, copy, move) the management system command files that are used to invoke the cut-through to the EMS GUI clients or the NE CITs.

Related information

See the following topic in this document:

- "Cut Through Concepts" (p. 4-2)
- "Command Files for the Cut-Through" (p. 4-4)

Before you begin

Follow the order of task execution that is specified in "Order of task execution for cut-through" (p. 4-3).

Task

Complete the following steps to customize (edit, copy, move) the management system command files that are used to invoke the cut-through to the EMS GUI clients or the NE CITs.

1 For EMS GUI client and NE CIT cut-throughs, use Notepad or Wordpad to edit the **C:\cutthru.txt** file. Refer to "cutthru.txt file" (p. 4-4) for details. Save your changes.

2 If you need special launch settings for the Navis® EMS (SNMS) GUI client, go to Step 3.

If you need special launch settings for the ITM-SC GUI client, go to Step 4.

If you need special launch settings for the NE CITs, go to Step 5.

3 If you need special launch settings for the Navis® EMS (SNMS) GUI clien, use Notepad or Wordpad to edit the **C:\cutthruSNMS.bat** file. Refer to "cutthru.bat file" (p. 4-6) for details. Save your changes.

4 If you need special launch settings for the ITM-SC GUI client, use Notepad or Wordpad to edit the **C:\cutthruSC.bat** file. Refer to "cutthru.bat file" (p. 4-6) for details. Save your changes.

5 If the NE CIT software has been moved to a new location, delete, if necessary, the **C:\cutthru_UNIE_CIT.bat** or **C:\cutthru_LX_CIT.bat** file. Refer to "cutthru.bat file" (p. 4-6) for details.

6 If the CIT software does not contain the particular **Launch.bat** (**LaunchUniteGUI.bat** or **OMS-LaunchXtremeGUI.bat**file), obtain this file from the OMS host at the following URL:

https://<OMS host IP address>/CITDATA

Put the particular **Launch.bat** file in the root directory of the CIT software.

If the CIT software has been moved to a new location, move the **Launch.bat** file. Refer to "Launch file" (p. 4-6) for details.

END OF STEPS

Cut-Through from OMS GUI to NMA GUI for Port Provisioning

Overview

This section contains conceptual information about configuring the Java policy files, installing the Network Management Adapter (NMA) GUI software on PC and customizing OMS GUI configuration files that are used to invoke the cut-through to the Network Management Adapter (NMA) GUI Port pages for port provisioning purpose.

> **Important!** The NMA-cutthru to NMA is only applicable for 1671 Service Connect (SC) NEs port provisioning.

Before you begin

Before launching Network Management Adapter (NMA) GUI, configure your PC as per the following steps:

1. Install the NMA GUI software on PC.
2. Configure the Java Policy file.
3. Customize OMS GUI Configuration files.

Related information

See the following topics in this document:

- "Cut Through Concepts" (p. 4-2)

Cut-through to NMA GUI for Port Provisioning

When the 1671 Service Connect (SC) NEs are added to the OMS system, you can provision the facility ports of these network elements by cut-through from the OMS Port Page to the NMA Port Pages.

The OMS Port Page has two options to cut-through:

- **Add port**- will go to the NMA top page of the facility domain.
- **Display and provision port** - will go to the NMA specific port page.

You may navigate to other ports of the same NE in two ways:

- By selecting another port on the opened NMA Port Page.
- By selecting another port on the OMS Port Page.

You may cut-through to multiple NMA GUI Port Pages with each page associated to a username and a network element. You may exit each of these NMA GUI Port Pages individually and re-open it.

> **Important!** Do not attempt to abort a NMA GUI Port Page until it is fully displayed. When you exit OMS GUI and close the browser, all opened NMA GUI Port Pages will be automatically closed.

Install the NMA GUI Software

Each release of NMA GUI software is backward compatible to its previous releases. Under normal circumstances, we suggest you install the latest release of the NMA GUI software and eliminate the previous releases. Obtain the NMA GUI self installation package, file **Setup.exe**, click on the file and the software package will install itself at **C:\ALU**.

> **Important! C:\ALU** is the only valid directory to store the NMA GUI software. Do not attempt to install or move the NMA GUI software to another directory.

Policy File Configuration to Launch NMA GUI

Refer to“Configure the java.policy File for Cut-Through” (p. 4-25) task for detailed instructions.

Customize OMS GUI Configuration Files

There are three files that enables and governs the NMA GUI launching. Once you specify the java policy file to give OMS GUI permission to access these files , by default, you may ignore these files. Only under some special circumstances, you may need to redefine the value of some parameters in *cutthru.txt.*

The three files are as follows:

1. **C:\cutthru.txt** is a text file that contains the configuration parameters to administer the cut-through at special circumstances. Modify the "debug" parameter to "true" to turn on the traces for debugging. This file is automatically generated by OMS GUI if it does not previously exist on your PC. If your PC already has this file created and it is out of date, then you need to remove (or rename) it so the new version will be generated for you. If you have your own patches in the previous file that you want to carry on, then you would need to port them over (from the renamed file) to the newly generated file. The values of the parameters will take effect at the next cut-through request.
2. **C:\cutthruEMA.bat** is the batch file automatically generated by OMS GUI to incorporate the execution to the launching directory and parameters. You should never modify the content of this file.
3. **C:\ALU\OMS_EMA\script\launchEMA.bat** is the batch file used to invoke the NMA GUI passing parameters needed to communicate with the target NMA server. This file is automatically populated when the NMA GUI is installed at your PC. The location of the file is **C:\ALU\OMS_EMA\script.**

5 Licensing

Overview

Purpose

This chapter contains conceptual information and tasks about licenses.

Contents

The Management System and Its Licensing Function

The function of a license

A license verifies that a customer on a particular supported platform (Server Platform or PC Platform) has purchased and can rightfully use OMS and related OMS features and/or software on that particular platform.

Licenses and the platform on which OMS is installed

The "OMS_CORE license" (p. 5-5) supports both the Server Platform and the PC Platform.

The types of licenses that are offered with OMS for licensed features are dependent on whether the management system is installed on its Server Platform or its PC Platform. The actual size and the processing power of the Server Platform does not restrict any currently supported OMS feature license; however, the size and the processing power of the PC Platform does restrict the types of feature licenses that it supports.

Examples:

The "OMS_CORE license" (p. 5-5) can be installed on both the Server Platform and the PC Platform; however, the "OMS_DET license" (p. 5-6), which is the license for the Data Extraction tool, can only be installed on the Server Platform.

In addition, certain licenses, such as the "OMS_TMF license" (p. 5-15) and "OMS_NB_SNMP license" (p. 5-10), have other restrictions. On the Server Platform, both licenses can be installed. On the PC Platform, only one license can be installed.

Licenses and user role profiles

The licenses that are installed for the management system govern the types of tasks that are available for use in the user role profiles. For example: a management system that does not have a license for the Ethernet Management feature ("OMS_EM license" (p. 5-7)) does not make the Ethernet Non-Switched Service Provisioning task available for the NOC Expert Operator.

For a complete list of all tasks and their associated licenses, see "User Tasks" (p. 7-7) or see "Available Licenses" (p. 5-4) for the details regarding a particular license.

Licenses and the graphical display

The installation of some licenses control the graphical display of the management system.

As its name implies, the installation of the "OMS_CORE license" (p. 5-5) enables most icons and object links that control core management system functions and features. The installation of additional licenses further enables the graphical display of the management system. For example: activation of the "OMS_TMF license" (p. 5-15) enables the display of the **OMS-OS Connections** page, which is a part of **Management Network**. However some licenses, such as the "OMS_DR license" (p. 5-7) license, do not have any affect on the graphical display of the management system.

For an explanation of how each license affects the graphical display of the management system, see the description of the license, which can be found in "Available Licenses" (p. 5-4).

Licenses and upgrades to new revisions of the management system

The type of upgrade that is being made determines whether new licenses are required.

A major revision of the management system is one that is identified as Rx.y.

For example: R5.0 was a major revision of the management system.

A minor revision of the management system in one that is identified as Rx.y.z.

For example: R5.0.1 was a minor revision of the management system.

Upgrades between major revisions of the management system require a new set of license keys.

For example: an upgrade from R5.0 to R6.0 would require a new set of license keys.

Upgrades between major revisions of the management system to the next logical minor revisions of the management system do not require new licenses keys, except if new features is being added.

For example: R5.0 to R5.0.1 would not require a new license key. However, if the Ethernet Management Feature was not purchased and therefore not licensed in R5.0 and was needed in R5.01 or R5.0.2, then the feature would have to be purchased for R5.01 or R5.0.2 and the license keys, which would be *new* to the existing R5.0 management system installation, would be required.

In addition, upgrades between minor revisions of the management system to the next logical minor revision version of the management system do not require new licenses keys, except if new features is being added.

For example: Rx.y.z1 to Rx.y.z2

The License pages

Most licenses are installed during the installation of the management system; however, the management system also supports licensing functions from its **Administration > Licenses** pages for some licenses that must be installed on the HP® server on which the management system is currently running.

The OMS permits system administrators to use the Licenses page to do the following:

- View a list of licenses installed on the application server; refer to the "View a List of Licenses" (p. 5-17) task for details.
- Add a license; refer to the "Add a License" (p. 5-18) task for details.

  Note that the "Add a License" (p. 5-18) task cannot be used to add the following licenses, which must be added during installation time:

  - "OMS_CORE license" (p. 5-5)
  - "OMS_GWS license" (p. 5-8)
  - "OMS_NA license" (p. 5-9)
  - "OMS_PM_SERVER license" (p. 5-12)

The two License pages display the following information:

- The *license name* is the character string in which the system identifies the license. Refer to "Available Licenses" (p. 5-4) for a list of the licenses that the management system supports for its operating environments.
- The *value* is a number <number> or <n> that represents a specific quantity. Refer to "OMS_CORE license" (p. 5-5), "OMS_NE license" (p. 5-10), "OMS_NA license" (p. 5-9), and "OMS_UD license" (p. 5-16) for details.
- The *license key*, which is required when a license is added to the management system on the Add License page, is an encrypted 1 to 100 ASCII character string that includes the host server ID.

License-related platform alarms

The following hot link provides additional information on a platform alarm that could be related to the malfunctioning of a license: "NE_LICENSE_EXCEEDED" (p. 42-21).

Available Licenses

OMS_BPM license

The OMS_BPM license enables the management system to support Bulk Performance Monitoring (BPM) data collection, which is the ability to collect performance data on all monitored TPs in the network.

The OMS_BPM license can only be installed on the Server Platform; it cannot be installed on the PC Platform. This license is required only on the HP® server on which the management system is running.

For the successful operation of BPM, OMS_BPM must be installed on the server on which the management system resides. If BPM is to reside on a dedicated server, the "OMS_PM_SERVER license" (p. 5-12) is required on the BPM dedicated server.

The "OMS_PM_SERVER license" (p. 5-12) must be installed during the initial installation of the distributed BPM server. It cannot be added with the "Add a License" (p. 5-18) task.

Note: If the OMS_BPM license is not installed, the system defaults to TP Mode for performance monitoring. For more information about TP mode and BPM mode, refer to the *OMS Service Assurance Guide*.

The OMS_BPM license does not control the functioning of any user task; however, the OMS_BPM license does control the display of the Performance Measurements Points page. Refer to the discussion in the "BPM" (p. 11-6) section of this document, the "OMS_PM_SERVER license" (p. 5-12), and the *OMS Service Assurance Guide* for additional details.

OMS_CORE license

The OMS_CORE license enables the basic OMS (the management system) in the SONET and SDH environments. In addition, the OMS_CORE license enables the management system application on any combination of network adapters (NAs) on the main server. The user designates the choice of TNA (TL1), CNA (CMISE) or NMA (1671 Service Connect (SC) NEs) during system installation/configuration.

Important! Without the OMS_CORE license, the management system cannot be brought up. As such, the OMS_CORE license cannot be added through the administration pages of the management system; meaning, it cannot be added using the "Add a License" (p. 5-18) task.

The OMS_CORE license can be installed on the Server Platform and on the PC Platform.

The following is the format of the OMS_CORE license:

OMS_CORE <number>

Where: **number** specifies the number of CPUs that are licensed. The system obtains the **number** of CPUs from the license key and displays this number to the user. Manual entry of this number is not required.

The OMS_CORE license controls the following user tasks:

- "Alarm Observation user task" (p. 7-7) and "Alarm Supervision user task" (p. 7-7)
- "All User Activity Log user task" (p. 7-8)
- "All TL1 Macro Files Management user task" (p. 7-7)
- "Area and Aggregate Management user task" (p. 7-8) and "Area and Aggregate Management (View Only) user task" (p. 7-8)
- "Connection Management user task" (p. 7-9) and "Connection Management (View-Only) user task" (p. 7-9)
- "Database Back Up Administration user task" (p. 7-10) and "Database Back Up Administration (View-Only) user task" (p. 7-10)
- "Fault Management Logs Administration user task" (p. 7-14)
- "Ethernet Element Management user task" (p. 7-11) and "Ethernet Element Management (View-Only) user task" (p. 7-12)
- "Global UI Settings user task" (p. 7-14)
- "Login Session Administration user task" (p. 7-14)
- "My Preferences user task" (p. 7-15)
- "NE Engineering user task" (p. 7-15) and "NE Engineering (View-Only) user task" (p. 7-16)
- "NE Management user task" (p. 7-17) and "NE Management (View-Only) user task" (p. 7-17)
- "NE Management Access user task" (p. 7-16)

- "NE Software Management user task" (p. 7-17) and "NE Software Management (View-Only) user task" (p. 7-18)
- "OMS ASAP Management user task" (p. 7-18)
- "Own Administration user task" (p. 7-18)
- "Own TL1 Macro Files Management user task" (p. 7-18)
- "Own User Activity Log user task" (p. 7-19)
- "Performance Monitoring user task" (p. 7-19) and "Performance Monitoring (View-Only) user task" (p. 7-19)
- "Profile Management user task" (p. 7-20)
- "Profile Management (View Only) user task" (p. 7-21)
- "Security Log user task" (p. 7-21)
- "SHDSL Device Password Modification user task" (p. 7-21)
- "System Administration user task" (p. 7-21)
- "System Alarm Supervision user task" (p. 7-22)
- "User Administration user task" (p. 7-22)

As its name implies, the installation of the OMS_CORE license enables most icons and object links that control core management system functions and features. In addition, the OMS_CORE license also enables the execution of the In-service Upgrade tool; see Chapter 25, "NE In-Service Upgrade" for details.

OMS_DET license

The OMS_DET license enables the Data Extraction command line tool for the SONET operating environment. See Chapter 16, "Data Extraction" for details.

The OMS_DET license does not control the functioning of any user task. In addition, the OMS_DET license does not enable any icon or object link that controls any management system function or feature.

The OMS_DET license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_DET license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_DP license

The OMS_DP license enables the Domain Partitioning feature, which is a partitioning of network resources, which specifically are entire NEs, into domains and the ability to restrict a user's access based on these partitions.

The OMS_DP license controls the functioning of the "Domain Partitioning Management" (p. 1-11).

The installation of the OMS_DP license enables the following in the management system:

- the Domains List
- the Domain attribute in the NE/Port Assignment list
- the viewing ability of all NEs, Areas, and/or Aggregates for all users
- the representation of the domain on the graphical layout
- the representation of the domain on the Network Map

The OMS_DP license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_DP license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_DR license

The OMS_DR license enables Disaster Recovery in the SONET and SDH environments. See "Disaster Recovery Concepts" (p. 20-2) for details.

The OMS_DR license does not control the functioning of any user task. In addition, the OMS_DR license does not enable any icon or object link that controls any management system function or feature.

The OMS_DR license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_DR license cannot be added using the "Add a License" (p. 5-18) task. The OMS_DR license must be added during the installation of the system. If the OMS_DR license was not installed during the initial installation of the management system, a *scratch* installation is then needed.

OMS_EM license

The OMS_EM license enables the Ethernet Management feature in the SONET and SDH environments. See the *OMS Ethernet Management Guide* for details about this feature.

The OMS_EM license controls the following user tasks:

- "Ethernet Administration user task" (p. 7-11)
- "Ethernet Hub-and-Spoke Service Provisioning user task" (p. 7-12)
- "Ethernet Infrastructure Provisioning user task" (p. 7-12)
- "Ethernet Non-Switched Service Provisioning user task" (p. 7-13)
- "Ethernet Switched Service Provisioning user task" (p. 7-13)
- "Ethernet (View-Only) user task" (p. 7-13)

The installation of the OMS_EM license enables the graphical display of the following icons and object links that control management system functions and features:

- Within the **Network Elements** section of the management system, the OMS_EM license controls **Link Aggregation Groups**.
- Within the **Connections** section of the management system, the OMS_EM license controls **Ethernet Orders** and **Ethernet Services**.
- From the **Display Route** icon on the Network Map, the OMS_EM license enables the display of the Ethernet service and Ethernet VSN menu items.
- From the **New** icon on the Network Map, the OMS_EM license enables the display of the Ethernet menu items.

The OMS_EM license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_EM license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_GWS license

The OMS_GWS license enables the software on each distributed GUI web server (GWS).

The OMS_GWS license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

An OMS_GWS license is needed on each separate distributed GUI web server. An OMS_GWS license is not needed on the main application server. As such, the OMS_GWS license cannot be added through the administration pages of the management system; meaning, it cannot be added using the "Add a License" (p. 5-18) task. The OMS_GWS license must be added during the installation of the system.

For additional details on distributed architecture, refer to Chapter 11, "Co-Resident and Distributed Architectures".

The following is the format of the OMS_GWS license:

OMS_GWS <number>

Where: **number** specifies the number of CPUs that are licensed on the distributed GUI web server.

The OMS_GWS license does not control the functioning of any user task. In addition, the OMS_GWS license does not enable any icon or object link that controls any management system function or feature.

OMS_HOTDR license

The OMS_HOTDR license enables the High Availability feature for the SONET operating environment. See Chapter 21, "High Availability" for details.

The OMS_HOTDR license does not control the functioning of any user task. In addition, the OMS_HOTDR license does not enable any icon or object link that controls any management system function or feature.

The OMS_HOTDR license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_HOTDR license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_MTOSI license

The OMS_MTOSI license enables the Multi-Technology Operations System Interface (MTOSI), which is a northbound Extensible Markup Language (XML) interface from OMS that conforms to the TMF814 Northbound Interface Standards for MTOSI. See Chapter 19, "MTOSI" for details.

The functioning of MTOSI requires the OMS_MTOSI license along with the "OMS_TMF license" (p. 5-15).

The OMS_MTOSI license does not control the functioning of any user task. In addition, the OMS_MTOSI license does not enable any icon or object link that controls any management system function or feature.

The OMS_MTOSI license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_MTOSI can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_NA license

The OMS_NA license enables any supported combination of network adapters (NAs) on distributed servers only.

The OMS_NA license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

NA licenses are needed on any platform that is running the NA application in the SONET or SDH environments. As such, the OMS_NA license cannot be added through the administration pages of the management system; meaning, it cannot be added using the "Add a License" (p. 5-18) task. The OMS_NA license must be added during the installation of the system and, at which time, the user can designate the choice of TNAs (TL1 network adapters) or CNAs (CMISE network adapters).

The following is the format of the OMS_NA license:

OMS_NA <number>

Where: **number** specifies the number of CPUs that are licensed. The system obtains the **number** of CPUs from the license key and displays this number to the user. Manual entry of this number is not required.

The OMS_NA license does not control the functioning of any user task. In addition, the OMS_NA license does not enable any icon or object link that controls any management system function or feature.

OMS_NB_SNMP license

The OMS_NB_SNMP license enables the northbound Simple Network Management Protocol (SNMP) interface. For details about the feature, refer to "SNMP Interface" (p. 17-5).

The OMS_NB_SNMP license does not control the functioning of any user task. In addition, the OMS_NB_SNMP license does not enable any icon or object link that controls any management system function or feature.

The OMS_NB_SNMP license can be installed on the Server Platform and on the PC Platform.

The OMS_NB_SNMP license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_NE license

The OMS_NE license enables the addition of an NE type up to a specified limit.

The following is the format of the OMS_NE license:

OMS_NE_<type> <number>

Where: **type** represents one of the NE type specified in the following table and **number** specifies the maximum number of the NE type that is allowed in the management system.

The OMS_NE license can be installed on the Server Platform and on the PC Platform.

The OMS_NE license can be added to the management system using the "Add a License" (p. 5-18) task.

The following table summarizes each NE and license name.

Important! Each release of OMS supports certain NEs within Alcatel-Lucent's family of optical NEs. Mention of NEs in the text of this document that are not supported in this particular release of the management system apply to prior and/or future releases of the management system.

NE License[1]	NE Type[1]
OMS_NE_ADMC	1643 ADM MultiService Mux (Compact Shelf)

NE License[1]	NE Type[1]
OMS_NE_ADMU	1663 Add Drop Multiplexer (ADMu)
OMS_NE_ADM16	WaveStar® ADM 16/1
OMS_NE_ADM4	WaveStar® ADM 4/1
OMS_NE_AM	1643 Access Multiplexer (AM)
OMS_NE_AM1	WaveStar® AM 1
OMS_NE_AMC	1645 Access Multiplexer Compact (AMC)
OMS_NE_AMS	1643 Access Multiplexer Small (AMS)
OMS_NE_AMU	1655 Access Multiplexer Universal (AMU)
OMS_NE_BWM	WaveStar® Bandwidth Manager
OMS_NE_CBG	CBGX is an indirectly managed NE that provides a cut-through to the Navis® EMS-CBGX system.
OMS_NE_DACS4	WaveStar® DACS 4/4/1
OMS_NE_DDMOC3	DDM-2000 OC3 Multiplexer
OMS_NE_DMX	1665 DMX Access Multiplexer
OMS_NE_DMXPLORE	1665 Data Multiplexer Explore (DMXplore)
OMS_NE_DMXTEND	1665 DMXtend Access Multiplexer
OMS_NE_EON[2]	1694 Enhanced Optical Networking (EON)[2]
OMS_NE_ISMADM	ISM ADM 1 and ISM ADM 4
OMS_NE_ISMRPTR	ISM Repeater
OMS_NE_ISMTM	ISM TM 1 and ISM TM 4
OMS_NE_LU	1675 Lambda Unite MultiService Switch (MSS)
OMS_NE_LX[2]	1625 LambdaXtreme® Transport[2]
OMS_NE_PHASEADM	PHASE ADM 4/4 and PHASE ADM 16/4
OMS_NE_PHASELR	PHASE LR 4 and PHASE LR 16
OMS_NE_PHASELXC	PHASE LXC 4/1 and PHASE LXC 16/1
OMS_NE_PHASETM	PHASE TM 4/4 and PHASE TM 16/4
OMS_NE_OLS16T	WaveStar® OLS 1.6T

NE License[1]	NE Type[1]
OMS_NE_SLM	Includes the entire SLM-family of NEs: •SLM ADM 16 •SLM MS Protected TM 4 •SLM MS Protected TM 16 •SLM Regenerator 4 •SLM Regenerator 16 •SLM Unprotected TM 4 •SLM Unprotected TM 16
OMS_NE_TDM10G	WaveStar® TDM10G (STM-64)
OMS_NE_WSM[2]	1695 Wavelength Services Manager (WSM)[2]

[1] Refer to the "Summary of supported NEs" (p. 1-5) to determine if the NE is supported in this release of the management system.

[2] The Repeater for this NE does not have a separate license.

OMS_NETINV license

The OMS_NETINV license enables the Network Inventory Extraction tool in the SONET and SDH operating environments. Also, the OMS_NETINV license allows XML-based external interfaces to enable planning systems such as VPI, RSoft, 1625 LambdaXtreme® Transport Engineering and Planning Tool (EPT), and DNA. See "Set Up 1625 LambdaXtreme® Transport EPT Communication" (p. 43-5) and Chapter 23, "Network Inventory Extraction" for details.

The OMS_NETINV license does not control the functioning of any user task. In addition, the OMS_NETINV license does not enable any icon or object link that controls any management system function or feature.

The OMS_NETINV license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_NETINV license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_PM_SERVER license

The OMS_PM_SERVER license is required if the OMS_BPM feature is deployed on a separate server; meaning, this license is needed on that server in what is known as a *distributed configuration*. As such, the OMS_PM_SERVER license cannot be added through the administration pages of the management system; meaning, it cannot be added using the "Add a License" (p. 5-18) task. The OMS_PM_SERVER license must be added during the installation of the system.

The OMS_PM_SERVER license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The following is the format of the OMS_PM_SERVER license:

OMS_PM_SERVER <number>

Where: **number** specifies the number of CPUs that are licensed on the particular server. The system obtains the **number** of CPUs from the license key and displays this number to the user. Manual entry of this number is not required.

The OMS_PM_SERVER license does not control the functioning of any user task. In addition, the OMS_PM_SERVER license does not enable any icon or object link that controls any management system function or feature. Refer to the "OMS_BPM license" (p. 5-4) and the *OMS Service Assurance Guide* for additional details.

OMS_PREPLAN license

The OMS_PREPLAN license enables the Preplan Restoration feature, which reserves and dedicates bandwidth in order to preplan the restoration of a system. It replaces the traditional protection methods of having reserved dedicated fiber links or bandwidth on existing fiber links.

The OMS_PREPLAN license functions in conjunction with the following installation parameters:

- "Alarm Triggered Preplan Restoration" (p. 6-160)
- "Automatic Routing of Preplan Restoration Connections" (p. 6-161)

The OMS_PREPLAN license controls the functioning of the following user tasks:

- "Preplan Management user task" (p. 7-20)
- "Preplan Management (View Only) user task" (p. 7-20)

In addition, the OMS_PREPLAN license enables the Preplan Connections icon and subsequent object links that control management system functions and features.

The OMS_PREPLAN license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_PREPLAN license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_RCF license

The OMS_RCF license controls the fault analysis functioning and the root cause failure (RCF) analysis functioning of various user tasks, along with icons and/or object links on the management system interface.

The OMS_RCF license enables the icon or object link for Root Cause Failures. In addition, the OMS_RCF license enables the link alarm on the Network Map and on the graphical layout.

The OMS_RCF license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_RCF license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_ROUTING license

The OMS_ROUTING license enables Auto Routing and Constrained Auto Routing for network connection provisioning in the SONET operating environment.

The OMS_ROUTING license does not control the functioning of any user task. However, activation of the OMS_ROUTING license enables the **Automatic** option in the Routing field of the network connection provisioning forms.

The OMS_ROUTING license can be installed on the Server Platform and on the PC Platform.

The OMS_ROUTING license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_SG license

The OMS_SG license enables Serviceguard, which is HP®'s high availability (HA) clustering solution.

The OMS_SG license does not control the functioning of any user task. In addition, the OMS_SG license does not enable any icon or object link that controls any management system function or feature.

The OMS_SG license can be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_SG license cannot be added using the "Add a License" (p. 5-18) task. The OMS_SG license must be added during the installation of the system. If the OMS_SG license was not installed during the initial installation of the management system, a *scratch* installation is then needed.

OMS_TIM license

The OMS_TIM license enables the TMN Integration Module (TIM) for Northbound Interface support. See "TIM Interface for a Northbound OSS" (p. 17-3) for details.

The OMS_TIM license does not control the functioning of any user task. In addition, the OMS_TIM license does not enable any icon or object link that controls any management system function or feature.

The OMS_TIM license can be installed on the Server Platform and on the PC Platform.

The OMS_TIM license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_TL1_ALARM license

The OMS_TL1_ALARM license enables the Northbound TL1 Alarm Interface for SONET and SDH environments. See "Northbound TL1 Alarm Interface" (p. 17-1) for details.

The OMS_TL1_ALARM license does not control the functioning of any user task. In addition, the OMS_TL1_ALARM license does not enable any icon or object link that controls any management system function or feature.

The OMS_TL1_ALARM license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_TL1_ALARM license can be added to the management system using the "Add a License" (p. 5-18) task.

OMS_TMF license

The OMS_TMF license enables the TMF814 Northbound Interface. See Chapter 18, "TMF814 Northbound Interface" for details.

The OMS_TMF license controls the functioning of the "TMF Session Administration user task" (p. 7-22). In addition, activation of the OMS_TMF license enables the display of the **OMS to OS TMF Communication** page, which is a part of **Management Network**.

The functioning of the Multi-Technology Operations System Interface (MTOSI), which is a northbound eXtensible Markup Language (XML) interface from OMS that conforms to the TMF814 Northbound Interface Standards for MTOSI, requires the "OMS_MTOSI license" (p. 5-9) along with the OMS_TMF license. Refer to Chapter 19, "MTOSI" for details on this feature.

The OMS_TMF license can only be installed on the Server Platform; it cannot be installed on the PC Platform.

The OMS_TMF license can be added to the management system using the "Add a License" (p. 5-18) task. Once the OMS_TMF license has been added, it must be activated with the "Activate the TMF814 Northbound Interface License" (p. 18-20) task.

OMS_UD license

The OMS_UD license enables Non-Managed NE Support in both the SONET and SDH environments.

The following is the format of the OMS_UD license:

OMS_UD <number>

Where: **number** specifies the maximum number of non-managed NEs that are allowed in the management system.

If users attempt to add a non-managed NE when the number of non-managed NEs has already reached the system limit, the management system denies the request and issues an error message.

The OMS_UD license does not control the functioning of any user task. In addition, the OMS_UD license does not enable any icon or object link that controls any management system function or feature.

The OMS_UD license can be added to the management system using the "Add a License" (p. 5-18) task.

View a List of Licenses

When to use

Use this task to view a list of licenses.

Related information

See the following topic in this document:

- "The Management System and Its Licensing Function" (p. 5-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following step to view a list of licenses.

1 From the Administration home page, click on **Licenses**.

Result: The list of licenses is displayed.

END OF STEPS

Add a License

When to use

Use this task to add a license.

Related information

See the following topic in this document:

- “The Management System and Its Licensing Function” (p. 5-1)

Before you begin

The types of licenses that are offered with OMS are dependent on whether the management system is installed on its Server Platform or its PC Platform. Before attempting to add a license, refer to “Licenses and the platform on which OMS is installed” (p. 5-1).

Verify that you have the correct license name and license key.

This task cannot be used to add the following licenses, which must be added during installation time:

- “OMS_CORE license” (p. 5-5)
- “OMS_GWS license” (p. 5-8)
- “OMS_NA license” (p. 5-9)
- “OMS_PM_SERVER license” (p. 5-12)

Task

Complete the following steps to add a license.

1 From the Administration home page, click on **Licenses**.

Result: The Licenses page is displayed.

2 Click the **New** tool.

Result: The Add License page is displayed.

3 Complete the **License name** and **License key** fields and then click the **Submit** button.

Result: If the license name and key are valid, the management system outputs the following message and advises you to restart the system so the license features can take effect:

```
Operation completed successfully
```

If the license name or key is not valid, the management system displays the following message:

```
Attempt to add a license unsuccessful - <Invalid Name/Invalid
Key>
```

4 Restart the management system.

Result: The license features that were added are now fully activated.

END OF STEPS

6 The Application and Its Installation Parameters

Overview

Purpose

This chapter explains the concepts and the tasks required to modify installation parameters.

Contents

Installation Parameter Concepts

Definition

An installation parameter is a variable value that controls the behavior of a management system feature and that is set during the installation of the management system. For example, an installation parameter called *Connection Alias* controls whether the **Connection Alias** field appears on the Add Connection page.

An installation parameter is also known as a *system parameter*.

lt_param_reconfig and its menu options

Many of the installation parameters that control the behavior of the management system can be edited using the **lt_param_reconfig** command-line tool.

The **lt_param_reconfig** command-line tool is used to display all installation parameters and to modify certain installation parameters. The menu items that **lt_param_reconfig** displays are mapped to particular installation parameters, which the following table details.

Menu Item	Hot Link for Installation Parameter Details
1. "Log Management Variables" (p. 6-12)	1. "Enable Security Log" (p. 6-12) 2. "Security Log Retention Time Period" (p. 6-12) 3. "Enable User Activity Log" (p. 6-13) 4. "User Activity Log Retention Time Period" (p. 6-13) 5. "Enable NE Notification Log" (p. 6-14) 6. "NE Notification Log Retention Time Period" (p. 6-14) 7. "Enable Command Response Log" (p. 6-15) 8. "Command Response Log Retention Time Period" (p. 6-15) 9. "Enable User Activity Logging of Synchronizations" (p. 6-16)

Menu Item	Hot Link for Installation Parameter Details
2. “Fault Management Variables” (p. 6-17)	1. “FM Alarm Delete Option” (p. 6-17) 2. “FM Instantaneous Alarm Delete Age” (p. 6-17) 3. “FM Alarm Log Retention Time” (p. 6-18) 4. “FM Alarm Severity Terminology” (p. 6-18) 5. “FM Browser Default Beep On” (p. 6-19) 6. “FM Browser Default Number Beeps” (p. 6-19) 7. “FM Browser Default Popup” (p. 6-20) 8. “FM ONNS Reroute Display” (p. 6-20) 9. “FM Default Clear Hold Off” (p. 6-21) 10. “FM Enable Equipment Protection Switch Log” (p. 6-21) 11. “FM Enable TDM MSP Protection Switch Log” (p. 6-22) 12. “FM Enable MSSPRING Protection Switch Log” (p. 6-22) 13. “FM Enable Non-Switch Protection Switch Log” (p. 6-23) 14. “FM Enable TDM SNCP Protection Switch Log” (p. 6-23) 15. “FM Enable WDM SNCP Protection Switch Log” (p. 6-24) 16. “FM Enable Resilient Protection Ring Switch Log” (p. 6-24) 17. “FM Protect Switch Log Retention Time” (p. 6-25) 18. “FM TCA Log Retention Time” (p. 6-25) 19. “Show or Hide the RCF Overall Connection State” (p. 6-26) 20. “Show or Hide the RCF OMS Connection State” (p. 6-26) 21. “Process Affected TPS in AID Alarms” (p. 6-27) 22.“Use Service Affecting State Provided by NE” (p. 6-27) 23.“Suppressed Alarms Logging” (p. 6-28) 24. “SDH Probable Cause” (p. 6-28)

Menu Item	Hot Link for Installation Parameter Details
3. “Element Administration Variables” (p. 6-29)	1. “Central Office Separator Mode” (p. 6-29) “Central Office Number of Characters” (p. 6-29) “Central Office Separator Character” (p. 6-30) 2. “Auto Configuration Resync” (p. 6-30) 3. “Discover LAN NEs” (p. 6-31) 4. “NE Date/Time Sync” (p. 6-31) 5. “CMISE Time Drift Threshold” (p. 6-32) 6. “CMISE Time Requests” (p. 6-33) 7. “CMISE Max Mean Round Trip Time Offset” (p. 6-33) 8. “CMISE Max Round Trip Time Difference” (p. 6-34) 9. “CMISE Max Time Drift” (p. 6-34) 10. “TL1 Time Drift Threshold” (p. 6-35) 11. “TL1 Max Round Trip Time” (p. 6-35) 12. “TL1 NE Timezone Setting” (p. 6-35) 13. “CBGX-EMS User Name” (p. 6-36) 14. “CBGX-EMS Password” (p. 6-37) 15. “SSH Authentication Algorithm” (p. 6-37) 16. “Drop Communication to NE for new controller card ” (p. 6-37) 17.“Validate total NE count for CMISE Network Adaptor” (p. 6-38) 18. “Validate total NE count for TL1 Network Adaptor” (p. 6-38) 19.“Total NE count for CMISE Network Adaptor” (p. 6-38) 20.“Total NE count for TL1 Network Adaptor” (p. 6-39) 21.“Total NE count percentage for CMISE Network Adaptor” (p. 6-39) 22.“Total NE count percentage for TL1 Network Adaptor” (p. 6-39) 23. “Time Synchronization Service” (p. 6-40) 24. “Time Synchronization Offset” (p. 6-40) 25. “Time Synchronization Polling Period” (p. 6-41) 26. “Hide In Domain” (p. 6-41)

Menu Item	Hot Link for Installation Parameter Details
4. "Connection Variables" (p. 6-42)	1. "Connection Name Format" (p. 6-42) 2. "Auto Discovery Connection Name Format" (p. 6-42) 3. "Connection Name Separator" (p. 6-43) 4. "Connection Alias" (p. 6-43) 5. "Connection Scheduling" (p. 6-44) 6. "Quality of Service" (p. 6-44) 7. "Customer Priority" (p. 6-45) 8. "Disable Alarms During Provisioning" (p. 6-45) 9. "CTP Alarm Monitoring" (p. 6-46) 10. "Orphan Cross Connection Deletion Tool" (p. 6-46) 11. "ONNS Paths Auto Retrieval" (p. 6-47) 12. "ONNS Network Type" (p. 6-47) 13. "SNC Fail Policy" (p. 6-48) 14. "Show End Port Columns on Connection List" (p. 6-48) 15. "Enable Port User Label" (p. 6-49) 16. "Allow Delete, Convert, and Rollback on Correlated Cross Connects" (p. 6-49) 17. "CTP Address Format for Non-managed NEs" (p. 6-50) 18. "Enable ASAP Fields on Provisioning Panel" (p. 6-50) 19."Enable Display of Service State on Graphical Layout" (p. 6-51) 20. "Retain Black Box Cross Connections" (p. 6-51) 21. "Enable display of LTU ports" (p. 6-52) 22."Enable display of Protection Switch Status-Automatic" (p. 6-52) 23."Enable display of Protection Switch Status-Selectable" (p. 6-52) 24."Enable display of XC Loopbacks" (p. 6-53) 25."Enable triggering Network Connection" (p. 6-53) 26."Modify Route of an Inconsistent Connection " (p. 6-53)
5. "Ethernet Variables" (p. 6-54)	1. "Default Option for Spoke Level 2 Switching" (p. 6-54) 2. "Enable Automatic Deletion Of Empty VCGs" (p. 6-54)

Menu Item	Hot Link for Installation Parameter Details
6. "Order Handling Variables" (p. 6-55)	1. "Order Versioning" (p. 6-55) 2. "History Order Storage Time" (p. 6-55) 3. "Reuse Order Number" (p. 6-56) 4. "Retention Period for Failed Requests" (p. 6-56) 5. "Enable Deletion of Rearrange with Reinstate History Orders" (p. 6-56) 6. "Rearrange with Reinstate History Order Storage Time (Hours)" (p. 6-57) 7. "Default Stop Step" (p. 6-57) 8. "Default Preplan Restoration Stop Step" (p. 6-58)
7. Performance Management Variables	1. "PM 24 Hour Retention Threshold" (p. 6-59) 2. "PM 15 Minute Retention Threshold" (p. 6-59) 3. "PM Variables - PM Panel Settings - Network Connections" (p. 6-60) 4. "PM Variables - PM Panel Settings - VCGs" (p. 6-65) 5. "PM Variables - PM Panel Settings - Ethernet Non Switched Service" (p. 6-70) 6. "PM Variables - PM Panel Settings - Ethernet Switched Service" (p. 6-73) 7. "PM Variables - PM Panel Settings - Hub & Spoke Service" (p. 6-76) 8. "PM Variables - PM Panel Settings - Virtual Switch Network" (p. 6-80) 9. "PM Variables - PM Panel Settings - Control Plane Service" (p. 6-83) 10. "PM Variables - PM Panel UNI/BI Best Effort" (p. 6-86)
8. "System Variables" (p. 6-87)	1. "Date Format" (p. 6-87) 2. "Time Format" (p. 6-87) 3. "Time Zone" (p. 6-88) 4. "Map Background" (p. 6-88) 5. "Default Terminology (SONET/SDH)" (p. 6-89) 6. "Enable ONNS Feature" (p. 6-89) 7. "Default TP Name to Show" (p. 6-90) 8. "Terminology Choice" (p. 6-90) 9. "Scheduled Job Restart" (p. 6-91) 10."OV Server" (p. 6-91)

Menu Item	Hot Link for Installation Parameter Details
9. Data Extraction Variables	1. “Enable/Disable DET Report Cron” (p. 6-120) 2. “Data Extraction Variables for NE Report” (p. 6-92) 3. “Data Extraction Variables for Equipment Report” (p. 6-95) 4. “Data Extraction Variables for All Alarm Report” (p. 6-98) 5. “Data Extraction Variables for Active Alarm Report” (p. 6-102) 6. “Data Extraction Variables for Network Connection Report” (p. 6-106) 7. “Data Extraction Variables for PM 24 Hour Report” (p. 6-109) 8. “Data Extraction Variables for PM 15 Minute Report” (p. 6-113) 9. “Data Extraction Variables for Link Connection Report” (p. 6-116) 10. “Number of Retry for Push Mode” (p. 6-120) 11. “Retry Interval (Minutes) for Push Mode” (p. 6-121)
10. “User Services Management Variables” (p. 6-121)	1. “Password Aging Time” (p. 6-121) 2. “Password Warning Time” (p. 6-122) 3. “Password Period of Non Use” (p. 6-122) 4. “Session Inactivity Timeout Flag” (p. 6-123) 5. “Session Inactivity Timeout Period” (p. 6-123) 6. “Proprietary Agreement Warning Message Flag” (p. 6-123) 7. “Proprietary Agreement Warning File” (p. 6-124) 8. “User Name Minimum Length” (p. 6-124) 9. “User Name Maximum Length” (p. 6-125) 10. “User Password Minimum Length” (p. 6-125) 11. “User Password Maximum Length” (p. 6-126) 12. “Enable Access via CSL/SAGE” (p. 6-126) 13. “Enable Etrust Authentication” (p. 6-127) 14. “Enable Access from Metarnet” (p. 6-127) 15. “Navis® EMS (SNMS) cut-through login name” (p. 6-128) 16. “Navis® EMS (SNMS) cut-through password” (p. 6-128)

Menu Item	Hot Link for Installation Parameter Details
11. "NBI Variables" (p. 6-129)	1. "Health Check Interval" (p. 6-129) 2. "Ping NMS Interval" (p. 6-129) 3. "Naming Service" (p. 6-130) 4. "Secondary Naming Service" (p. 6-130) 5. "MLSN Policy" (p. 6-131) 6. "TMF SNC Operation" (p. 6-132) 7. "TMF Unmanaged Domain Support" (p. 6-132) 8. "TMF SNC End Point Rules" (p. 6-133) 9. "TMF SNC Naming" (p. 6-133) 10. "TMF G7 - Contained VCG Servers" (p. 6-134) 11. "TMF G7 - Reissue Alarms when Correlation Changes" (p. 6-134) 12. "TMF G7 - Enable TMF G7 Interface" (p. 6-135) 13. "TMF - Raise Alarms During Connection Provisioning" (p. 6-135) 14. "Use G7 CTP Naming Format on TMF814 Interface" (p. 6-136) 15. "ASIM - Enable Alarm Server interface " (p. 6-136) 16. "ASIM - EMS identifier " (p. 6-137) 17. "Drop connections ending at CTP of SHDSL PTP" (p. 6-137) 18. "ASIM - Forward physical alarms to AS" (p. 6-138)
12. "TIM Variables" (p. 6-138)	1. "TIM Username" (p. 6-138) 2. "TIM Password" (p. 6-139) 3. "TIM Timezone" (p. 6-139) 4. "TIM FM Filtering" (p. 6-140) 5. "TIM Heartbeat Interval" (p. 6-140) 6. "TIM Alarm Severity Terminology" (p. 6-141) 7. "TIM Synchronous Data Transmission Terminology" (p. 6-141) 8. "TIM Enable PSEs from Equipment Switch as Alarms" (p. 6-142) 9. "TIM Enable PSEs from MSSPRING Switch as Alarms" (p. 6-142) 10. "TIM Enable PSEs from RPR Switch as Alarms" (p. 6-143) 11. "TIM Enable PSEs from TDM HO SNCP Switch as Alarms" (p. 6-143) 12. "TIM Enable PSEs from TDM MSP Switch as Alarms" (p. 6-144) 13. "TIM Enable PSEs from WDM HO SNCP Switch as Alarms" (p. 6-144)

Menu Item	Hot Link for Installation Parameter Details
13. "Northbound SNMP Variables" (p. 6-145)	1. "SNMP Version" (p. 6-145) 2. "SNMP Address/Port Number" (p. 6-145) 3. "SNMP Security Name" (p. 6-146) 4. "SNMP Security Level" (p. 6-146) 5. "SNMP Authentication Protocol" (p. 6-147) 6. "SNMP Authentication Password" (p. 6-148) 7. "SNMP Privacy Protocol" (p. 6-148) 8. "SNMP Privacy Password" (p. 6-149)
14. "Southbound SNMP Variables" (p. 6-149)	1. "SNMP Security Name" (p. 6-149) 2. "SNMP Security Level" (p. 6-150) 3. "SNMP Authentication Protocol" (p. 6-150) 4. "SNMP Authentication Password" (p. 6-151) 5. "SNMP Privacy Protocol" (p. 6-151) 6. "SNMP Privacy Password" (p. 6-152)
15. "External Authentication Variables" (p. 6-153)	1. "Authentication Method" (p. 6-153) 2. "Allow Local GUI User Authentication " (p. 6-153) 3. "Default User Role" (p. 6-153) 4. "Default User Domain" (p. 6-154) 5. "Authentication Server Retries" (p. 6-154) 6. "Authentication Server Timeout in Seconds" (p. 6-155) 7. "Authentication Server Selection Policy" (p. 6-155) 8. "Address of External Server 1" (p. 6-156) 9. "Shared Secret for Server 1" (p. 6-156) 10. "Address of External Server 2" (p. 6-157) 11. "Shared Secret for Server 2" (p. 6-157) 12. "Address of External Server 3" (p. 6-158) 13. "Shared Secret for Server 3" (p. 6-158) 14. "Address of External Server 4" (p. 6-159) 15. "Shared Secret for Server 4" (p. 6-159) 16. "Vendor Private Enterprise Number" (p. 6-160)

Menu Item	Hot Link for Installation Parameter Details
16. "Preplan Restoration Variables" (p. 6-160)	1. "Alarm Triggered Preplan Restoration" (p. 6-160) 2. "Automatic Routing of Preplan Restoration Connections" (p. 6-161) 3. "Preplan log retention period in days" (p. 6-161) 4. "Number of Retained History Orders" (p. 6-162) 5. "Hold Off Time for Alarm Triggered Restoration" (p. 6-162) 6."Maximum number of member pairs per plan" (p. 6-163) 7. "Maximum number of plans per preplan group" (p. 6-163)
17. Display Current Values	Displays all current values for fixed, reconfigurable, and dynamic installation parameters.

Modification of installation parameters

Each installation parameter has an optional value or values that can be specified in place of the value that was specified when the management system was installed. The behavior of the installation parameters can be modified with the "Modify an Installation Parameter" (p. 6-167) task.

Typically, modifying the installation parameters consists of one of these types of changes:

- Enabling or disabling an installation parameter by specifying values such as ON or OFF, 0 or 1, or TRUE or FALSE to indicate either functional state.
- Tuning an installation parameter by specifying a specific value within a range of values such as 0 to 3600 seconds; or 1 day to 30 days; or 10,000 to 200,000 records.
- Controlling the format that an installation parameter is to use by specifying a value within a choice of values such as TELCORDIA, M1400, or FREE_FORMAT.
- Entering a value for a password. The value is not displayed on the screen while being entered. It is then encrypted. Only the encrypted value is viewable.
  Note: The encryption processing can cause a delay before the new entry is confirmed.

Restarting of and interaction with system components

The installation parameters require none or one of the following components of the OMS system to be restarted for the parameter value change to take effect:

- **None**, which does not require any system restart.
- **OMS**, which requires a restart of the application server software and also causes the **GWS** to restart.
- **GWS**, which requires a restart of only the GUI web servers.
- **NAs**, which requires a restart of only the network adapters.

- **BPM**, which requires a restart of bulk performance monitoring, if the PM server application resides on a separate server.
- **All** components, which requires a restart of the OMS application along with the network adapters (NAs).

The **lt_param_reconfig** tool informs the user of component restart requirements when the user exits the tool using its quit options. Users should not force the tool to exit using an operating system interrupt such as `control-c` because such an interrupt causes the final actions of the tool to be skipped and the restart requirements will not be provided.

Log Management Variables

Enable Security Log

The Enable Security Log installation parameter enables or disables the security log.

Valid values for this parameter are YES to enable the security log or NO to disable the security log. The default is YES.

Related platform alarms are "SL_NEARLY_FULL" (p. 42-26) and "SL_FULL" (p. 42-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Log Management Variables**, which is option 1, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.SL.ENABLE.

Security Log Retention Time Period

The Security Log Retention Time Period installation parameter specifies the number of days for which security log records are to be retained.

Valid values for this parameter are 1 to 45 days. The default is 31 days.

Related platform alarms are "SL_NEARLY_FULL" (p. 42-26) and "SL_FULL" (p. 42-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Log Management Variables**, which is option 1, number 2.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.SL.RETENTION.

Enable User Activity Log

The Enable User Activity Log installation parameter enables or disables the user activity log. For an explanation of how the User Activity Log affects Connection Auto Discovery, see "Connection Auto Discovery and the User Activity Log" (p. 22-3).

Valid values for this parameter are YES to enable the user activity log or NO to disable the user activity log. The default is YES.

Related platform alarms are "UTL_NEARLY_FULL" (p. 42-27) and "UTL_FULL" (p. 42-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Log Management Variables**, which is option 1, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.UAL.ENABLE

User Activity Log Retention Time Period

The User Activity Log Retention Time Period installation parameter specifies the number of days for which user activity log records are to be retained. For an explanation of how the User Activity Log affects Connection Auto Discovery, see "Connection Auto Discovery and the User Activity Log" (p. 22-3).

Valid values for this parameter are 1 to 45 days. The default is 31 days.

Related platform alarms are "UTL_NEARLY_FULL" (p. 42-27) and "UTL_FULL" (p. 42-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Log Management Variables**, which is option 1, number 4.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.UAL.RETENTION.

Enable NE Notification Log

The Enable NE Notification Log installation parameter specifies whether the NE notification log is to be enabled or disabled.

Valid values for this parameter are NO (disable) or YES (enable). The default is YES, which enables the NE Notification Log.

Related platform alarms are "NEL_NEARLY_FULL" (p. 42-22) and "NEL_FULL" (p. 42-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Log Management Variables** option, which is option 1, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.NL.ENABLE.

NE Notification Log Retention Time Period

The NE Notification Log Retention Time Period installation parameter specifies the time in days for which notification log records are to be retained.

Valid values for this parameter are 1 to 45 days. The default is 31 days, which is 1 month.

Related platform alarms are "NEL_NEARLY_FULL" (p. 42-22) and "NEL_FULL" (p. 42-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Log Management Variables** option, which is option 1, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.NL.RETENTION.

Enable Command Response Log

The Enable Command Response Log installation parameter specifies whether the Command Response Log should be enabled or disabled.

Valid values for this parameter are YES (enable) or NO (disable). The default is YES, which enables the Command Response Log.

Related platform alarms are "CR_NEARLY_FULL" (p. 42-10) and "CR_FULL" (p. 42-9).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Log Management Variables** option, which is option 1, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.CR.ENABLE.

Command Response Log Retention Time Period

The Command Response Log Retention Time Period installation parameter specifies the time in days for which Command Response Log records are to be retained.

Valid values for this parameter are 1 to 45 days. The default is 31 days, which is 1 month.

Related platform alarms are "CR_NEARLY_FULL" (p. 42-10) and "CR_FULL" (p. 42-9).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Log Management Variables** option, which is option 1, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.CR.RETENTION.

Enable User Activity Logging of Synchronizations

The Enable User Activity Logging of synchronization parameter enables the logging of network synchronization activity in the user activity log. For an explanation of how the User Activity Log affects Connection Auto Discovery, see "Connection Auto Discovery and the User Activity Log" (p. 22-3).

Valid values for this parameter are **YES** to enable the logging for synchronizations, which is the existing behavior of the previous OMS releases; or **NO** to disable the synchronizations logging for the purpose of improving the capacity of the user activity log for more important actions. The default is **YES**.

Related platform alarms are "UTL_NEARLY_FULL" (p. 42-27) and "UTL_FULL" (p. 42-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Log Management Variables**, which is option 1, number 9.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.UAL.LOG_DBSYNC.

Fault Management Variables

FM Alarm Delete Option

The FM Alarm Delete Option installation parameter specifies the option to use to delete persistent alarms.

Valid values for this parameter are UNACK_ACK, ACK, UNACK, and ENF_CLR_ACK. Where:

- Setting **ACK** automatically removes any acknowledged alarms that are cleared from the management system. Unacknowledged alarms that are cleared remain in the system until the user acknowledges them. After they are acknowledged, they are removed from the management system.
- Setting **ENF_CLR_ACK** forces the user to acknowledge a cleared alarm regardless of whether it was acknowledged when it was raised before it is removed from the management system.
- Setting **UNACK** automatically removes any unacknowledged alarm that was cleared from the management system. An alarm that was acknowledged when the clear was reported has to be acknowledged again by the user before it is removed from the management system.
- Setting **UNACK_ACK**, which is the default, automatically removes any alarm that is cleared from the management system regardless of its acknowledgement status. An alarm is removed immediately when it is cleared, which is the default that is set at installation.

When the management system is installed, it is set to delete acknowledged and unacknowledged alarms automatically when they are cleared.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_ALM_DEL_OPTION.

FM Instantaneous Alarm Delete Age

The FM Instantaneous Alarm Delete Age installation parameter specifies the number of days in which instantaneous alarms are to be purged when a current alarm purge occurs.

Valid values for this parameter are 0 to 31 days. The default is 1 day. A value of 0 disables the purge.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_INST_DEL_AGE.

FM Alarm Log Retention Time

The FM Alarm Log Retention Time installation parameter specifies the number of days for which historic root cause failure records are retained.

Valid values for this parameter are 1 to 45 days. The default is 31 days.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.ALM.RETENTION.

FM Alarm Severity Terminology

The FM Alarm Severity Terminology installation parameter specifies whether the severity of alarms to be displayed should be those whose severity is critical/major/minor/warning (CMMW) or those whose severity is prompt/deferred/information (PDI) only.

Valid values for this parameter are CMMW (critical/major/minor/warning) or PDI (prompt/deferred/information). The default is CMMW to support the X.733 standard or PDI to support the PDI standard.

To modify this installation parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM.ALM_SEV_TERMINOLOGY.

FM Browser Default Beep On

The FM Browser Default Beep On installation parameter specifies whether or not a beep is to be emitted to recognize new events.

Note: The setting of this installation parameter can be overridden by a user selection in the **Application Preferences** setting on the **Preferences** page in the management system. See the *OMS Getting Started Guide* for instructions on how to change preferences.

Valid values for this parameter are TRUE or FALSE. The default is TRUE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as BROWSER_FM_DEFAULT_BEEP_ON.

FM Browser Default Number Beeps

The FM Browser Default Number Beeps installation parameter specifies the number of beeps that are to be emitted to recognize new events.

Note: The setting of this installation parameter can be overridden by a user selection in the **Application Preferences** setting on the **Preferences** page in the management system. See the *OMS Getting Started Guide* for instructions on how to change preferences.

Valid values for this parameter are 1 beep, 2 beeps, 3 beeps, 4 beeps, 5 beeps, 6 beeps, 7 beeps, 8 beeps, 9 beeps, or continuous beeping. The default is 3 beeps.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables** option, which is option 2, number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as BROWSER_FM_DEFAULT_NUM_BEEPS.

FM Browser Default Popup

The FM Browser Default Popup installation parameter specifies whether or not a pop-up window is to appear to recognize new events.

Note: The setting of this installation parameter can be overridden by a user selection in the **Application Preferences** setting on the **Preferences** page in the management system. See the *OMS Getting Started Guide* for instructions on how to change preferences.

Valid values for this parameter are TRUE or FALSE. The default is TRUE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 7.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as BROWSER_FM_DEFAULT_POPUP.

FM ONNS Reroute Display

The FM ONNS Reroute Display installation parameter enables the processing and the display of Optical Network Navigator System (ONNS) reroute notifications.

Valid values for this parameter are NONE or DISPLAY_REROUTE. The default is NONE, which disables the processing and display of ONNS reroute notifications.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_ONNS_REROUTE.

FM Default Clear Hold Off

The FM Default Clear Hold Off installation parameter specifies the time, in seconds, for which an alarm must remain cleared before the clear is recognized.

Valid values for this parameter are 0 seconds to 300 seconds. The default is 10 seconds, which means that clear events are not suppressed.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 9.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_DEFAULT_CLEAR_HOLD_OFF.

FM Enable Equipment Protection Switch Log

The FM Enable Equipment Protection Switch Log installation parameter enables or disables the processing of equipment protection switch events (PSEs).

Valid values for this parameter are Yes and No. The default is No, which means that the processing of equipment PSEs is to be disabled initially.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 10.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_EQM.

FM Enable TDM MSP Protection Switch Log

The FM Enable TDM MSP Protection Switch Log installation parameter enables or disables the processing of Time Division Multiplexing Multiplex Section Protection (TDM MSP) protection switch events (PSEs).

Valid values for this parameter are Yes and No. The default is No, which means that the processing of TDM MSP protection switch events is to be disabled initially.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 11.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_TDM_MSP.

FM Enable MSSPRING Protection Switch Log

The FM Enable MSSPRING Protection Switch Log installation parameter enables or disables the processing of Multiplex Section - Shared Protection Ring (MSSRING) protection switch events (PSEs).

Valid values for this parameter are Yes and No. The default is No, which means that the processing of MSSRING protection switch events is to be disabled initially.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 12.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_MSSRING.

FM Enable Non-Switch Protection Switch Log

The FM Enable Non-Switch Protection Switch Log installation parameter enables or disables the processing of protection switch events from the 1675 Lambda Unite MultiService Switch (MSS) that do not cause protection switching.

Valid values for this parameter are YES and NO. The default is NO, which means that the processing of protection switch events from the 1675 Lambda Unite MultiService Switch (MSS) is to be disabled initially.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 13.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_NON_SWITCH.

FM Enable TDM SNCP Protection Switch Log

The FM Enable TDM SNCP Protection Switch Log installation parameter enables or disables the processing of Time Division Multiplexing (TDM) high order (HO) Subnetwork Connection Protection (SNCP) protection switch events (PSEs).

Valid values for this parameter are Yes and No. The default is No, which means that the processing of TDM HO SNCP protection switch events is to be disabled initially.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 14.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_TDM_HO_SNCP.

FM Enable WDM SNCP Protection Switch Log

The FM Enable WDM SNCP Protection Switch Log installation parameter enables or disables the processing of Wavelength Division Multiplexing (WDM) high order (HO) Subnetwork Connection Protection (SNCP) protection switch events (PSEs).

Valid values for this parameter are Yes and No. The default is No, which means that the processing of WDM HO SNCP protection switch events is to be disabled initially.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 15.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_WDM_HO_SNCP.

FM Enable Resilient Protection Ring Switch Log

The FM Enable Resilient Protection Ring Switch Log installation parameter enables or disables the processing of resilent packet ring (RPR) switch events.

Valid values for this parameter are YES, which enables the processing, or NO, which disables the processing. The default is NO.

Refer to the "TCA_LOG_PURGED" (p. 42-26) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 16.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

Related platform alarms are "CR_NEARLY_FULL" (p. 42-10) and "CR_FULL" (p. 42-9).

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_PSE_PROCESS_RPR.

FM Protect Switch Log Retention Time

The FM Enable Resilient Protection Ring Switch Log installation parameter specifies the time in days for which records are to be retained in the Threshold Crossing Alert (TCA) log.

Valid values for this parameter are 1 to 31 days. The default is 31 days, which is 1 month.

Important! ITM-SC managed NEs will continue to forward PSE events regardless of the setting of this installation parameter.

Refer to the "PSE_LOG_PURGED" (p. 42-25) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 17.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

Related platform alarms are "CR_NEARLY_FULL" (p. 42-10) and "CR_FULL" (p. 42-9).

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.PSE.RETENTION.

FM TCA Log Retention Time

The FM TCA Log Retention Time installation parameter specifies the time in days for which records are to be retained in the Threshold Crossing Alert (TCA) log.

Valid values for this parameter are 1 to 31 days. The default is 31 days, which is 1 month.

Refer to the "TCA_LOG_PURGED" (p. 42-26) platform alarm for additional related information.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 18.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

Related platform alarms are "CR_NEARLY_FULL" (p. 42-10) and "CR_FULL" (p. 42-9).

When specifying option 17, **Display Current Values**, this installation parameter appears as LOG.TCA.RETENTION.

Show or Hide the RCF Overall Connection State

The Show or Hide the RCF Overall Connection State installation parameter controls the calculation and display of the overall connection root cause failure (RCF) state.

Valid values for this parameter are HIDE to hide the overall RCF state or SHOW to display the overall RCF state.

The default is HIDE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 19.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_RCF_OVERALL.

Show or Hide the RCF OMS Connection State

The Show or Hide the RCF OMS Connection State installation parameter controls the calculation and display of the root cause failure (RCF) state for OMS connections.

Valid values for this parameter are HIDE to hide the display of the RCF OMS connection state or SHOW to display the RCF OMS connection state.

The default is HIDE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 20.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_RCF_OMS_STATE.

Process Affected TPS in AID Alarms

The Process Affected TPS in AID Alarms installation parameter controls whether affected termination points (TPs) on AID alarms should be processed. This installation parameter is only applicable to systems in which nodes are being indirectly managed using ITM-SC.

Valid values for this parameter are YES and NO.

The default is NO. When this installation parameter is set to YES, alarm processing performance might be reduced.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 21.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_AID_AFFECTEDTPS.

Use Service Affecting State Provided by NE

The Use Service Affecting State Provided by NE installation parameter defines whether the service affecting (SA) value used is provided by the NE or is derived from correlation.

Valid values for this parameter are YES, it is the SA value provided by the NE or NO it is an SA value that is derived from correlation.

The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Fault Management Variables**, which is option 2, number 22.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_USE_NE_SA_VALUE.

Suppressed Alarms Logging

The FM Suppressed Alarms Logging installation parameter enables or disables the platform alarm which indicates that alarms have been suppressed.

Valid values for this parameter are Enabled and Disabled. The default is Enabled.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 23.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_SUPPRESSED_ALARMS_LOGGING.

SDH Probable Cause

The FM SDH Probable Causes specific to Lamda unite NE's are enabled.

Valid values for this parameter are True and False. The default is False.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Fault Management Variables** option, which is option 2, number 24.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as FM_SDH_PROBABLECAUSE.

Element Administration Variables

Central Office Separator Mode

The Central Office Separator Character installation parameter specifies the method to use in order to obtain the central office (CO) name from the network element (NE) name.

Valid values for this parameter are First n Characters, First occurrence of the Separator Character, or Last Occurrence of the Separator Character. The default is First N Characters.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Element Administration Variables**, which is option 3, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.CO_SEPARATOR_MODE.

Central Office Number of Characters

The Central Office Number of Characters installation parameter specifies the first number of characters to be used for the CO definition. This parameter is only applicable if the Central Office Separator Mode is *First N Characters*.

Note: Changes are not retrospectively applied to the database; that is, the CO name remains as is.

Valid values for this parameter are 8, 9, 10, and 11. The default is 11.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Element Administration Variables**, which is option 3, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.CO_NUM_CHARS.

Central Office Separator Character

The Central Office Separator Character installation parameter specifies if the number of characters is not the criteria, then the separator character is to be used. This parameter is only applicable if the Central Office Separator Mode is *First Separator, Last Separator*.

Note: Changes are not retrospectively applied to the database; that is, the CO name remains as is.

Valid values for this parameter are **/ - _ .** The default is **/**, which is the forward slash.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Element Administration Variables**, which is option 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.CO_SEP_CHAR.

Auto Configuration Resync

The Auto Configuration Resync installation parameter specifies the policy to be used for automatic configuration resynchronizations.

Valid values for this parameter are OFF and ADD_ONLY. The default is ADD_ONLY, which means that a configuration resynchronization is automatically performed on NEs after they are added to the management system.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Element Administration Variables**, which is option 3, number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.AUTO_CONFIG_RESYNC.

Discover LAN NEs

The Discover LAN NEs installation parameter specifies whether the Subnetwork Discovery feature of the management system should automatically discover NEs that are interconnected through a LAN. Once this parameter is set, the value set is globally applied to all managed TL1-NEs. For a list of currently supported TL1 NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are YES or NO. The default is YES. When this parameter is set to NO, these NEs are ignored.

Important! If the LAN that is connecting the management system to the gateway NEs is also connected to devices that are not managed by the management system (such as routers), these devices may appear as unmanaged elements on the management system and they may require manual deleting. Setting the parameter to NO prevents this situation; however, the NEs on the LAN must then be manually added rather than automatically discovered.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 3.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DISCOVER_LAN_NES.

NE Date/Time Sync

The NE Date/Time Sync installation parameter specifies the policy to resynchronize the date and time on NEs.

Note: With the CMISE NEs, the date and time are automatically synchronized when the NE connects. With the TL1 NEs, the NE Date/Time Sync parameter can be used to enable the auto synchronization of the date and time when the NE connects.

Important! The proper operation of OMS features relies the date and time of all managed NEs being synchronized with the OMS application. The OMS supports a mechanism for keeping the date and time of all managed NEs synchronized with the OMS application. When the NE Date/Time Sync installation parameter is being used, we recommend that the date and time of the management system application be kept accurate using a mechanism such as Network Time Protocol (NTP). Other date/time synchronization mechanisms can be used as long as the date and time of management system application is kept synchronized with all managed NEs, including having all managed NEs in the same time zone as the management system application. If other management systems are supporting the same set of NEs managed by OMS, the date and time of these other management systems must be synchronized with the OMS host, including having OMS and these other management systems in the same time zone.

Valid values for this parameter are AUTO_ON_CONNECTION or MANUAL_ONLY. The default is AUTO_ON_CONNECTION, which means to synchronize automatically after the NE connects.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.NE_DT_SYNC.

CMISE Time Drift Threshold

The CMISE Time Drift Threshold installation parameter specifies the maximum difference in seconds between the management system time and the CMISE-managed NEs that is allowed before the NE date/time synchronization is attempted. Once this parameter is set, the value set is globally applied to all managed CMISE-NEs. For a list of currently supported CMISE NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 0 seconds to 300 seconds (5 minutes). The default is 60 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 5.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. With a distributed CNA server configuration, you must also restart the distributed CNA server. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_TIME_DRIFT_THRESHOLD.

CMISE Time Requests

The CMISE Time Requests installation parameter specifies the number of times (tries) that a CMISE-managed NE is requested for its current time. Once this parameter is set, the value set is globally applied to all managed CMISE-NEs. For a list of currently supported CMISE NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 1 time to 10 times. The default is 3 times. **Important!** A higher value establishes a more accurate drift measurement, but consequently, takes longer to perform.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 6.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. With a distributed CNA server configuration, you must also restart the distributed CNA server. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_TIME_REQUESTS.

CMISE Max Mean Round Trip Time Offset

The CMISE Max Mean Round Trip Time Offset installation parameter specifies the maximum mean round trip time (RTT) offset for CMISE NEs in seconds, which is the maximum for the mean round trip time less the minimum round trip time observed. Once this parameter is set, the value set is globally applied to all managed CMISE-NEs. For a list of currently supported CMISE NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 0 seconds to 5 seconds. The default is 1 second.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 7.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. With a distributed CNA server configuration, you must also restart the distributed CNA server. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_TIME_MAX_RTT_OFFSET.

CMISE Max Round Trip Time Difference

The CMISE Max Round Trip Time Difference installation parameter specifies the maximum round trip time (RTT) difference in seconds, which is the maximum difference allowed between the minimum and maximum round trip times observed. Once this parameter is set, the value set is globally applied to all managed CMISE-NEs. For a list of currently supported CMISE NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 0 seconds to 300 seconds (5 minutes). The default is 60 second.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 8.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. With a distributed CNA server configuration, you must also restart the distributed CNA server. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_TIME_MAX_RTT_DIFF.

CMISE Max Time Drift

The CMISE Max Time Drift installation parameter specifies the difference, in seconds between the management system system time and the NE time, which if exceed, causes a date/time synchronization regardless of any other parameters set. Once this parameter is set, the value set is globally applied to all managed CMISE-NEs. For a list of currently supported CMISE NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 0 seconds to 1200 seconds (20 minutes). The default is 300 seconds (5 minutes).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 9.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. With a distributed CNA server configuration, you must also restart the distributed CNA server. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_TIME_MAX_DRIFT.

TL1 Time Drift Threshold

The TL1 Time Drift Threshold installation parameter specifies the maximum difference in seconds between the management system time and the TL1-managed NEs that is allowed before the NE date/time synchronization is attempted. Once this parameter is set, the value set is globally applied to all managed TL1-NEs. For a list of currently supported TL1 NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 1 seconds to 999 seconds. The default is 15 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 10.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TL1_TIME_DRIFT_THRESHOLD.

TL1 Max Round Trip Time

The TL1 Max Round Trip Time installation parameter specifies the maximum allowed time in seconds for the round trip of an RTRV-HDR message to a managed TL1 NE. Once this parameter is set, the value set is globally applied to all managed TL1-NEs. For a list of currently supported TL1 NEs, refer to "Summary of supported NEs" (p. 1-5).

Valid values for this parameter are 1 seconds to 999 seconds. The default is 15 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 11.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TL1_TIME_MAX_RTT.

TL1 NE Timezone Setting

The TL1 NE Timezone Setting installation parameter specifies the timezone setting for TL1 NEs.

Valid values for this parameter are SERVER_TIME or UTC. The default is UTC.

Important Notes! For networks that include CMISE NEs, this installation parameter must always be UTC because CMISE NEs do not support anything else. For networks that include only TL1 NEs, the network can be set to use the same timezone setting as the server.

If the TL1 NE Timezone Setting parameter is set to SERVER_TIME, all NEs are set to the time zone of the server. We strongly recommend that the server time zone be set to a time zone without daylight savings time adjustments; otherwise, issues may be encountered in certain areas dependent on the NE time such as Fault Management and Performance Management. Also note that if a time zone with daylight savings time is provisioned for the server, when a daylight savings time transition occurs, the times at the NEs will not be automatically adjusted. It is the responsibility of the user to manually invoke or schedule a NE Date/Time Synchronization for all NEs in the network after the time in which the server is adjusted for a daylight savings time transition.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 12.

This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. In addition, the NA types do use this parameter; therefore, an automatic download of parameters to the NAs does occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Stop the NAs" (p. 9-12) and "Start the NAs" (p. 9-11) tasks for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NETWORK_TZ.

CBGX-EMS User Name

The CBGX-EMS User Name installation parameter defines the user name for the TMF814 connection to the Navis® EMS-CBGX system. For addition information on the Navis® EMS-CBGX system, refer to the "Install the NAVIS® EMS-CBGX System" (p. 4-16) task and the "OMS_NE license" (p. 5-10) (OMS_NE_CBG).

The default value for this parameter is superuser.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 13.

This parameter does not require any system restart (**None**) for the parameter values to take effect. Changes take effect at the next attempt to connect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_CBGX_USERNAME.

CBGX-EMS Password

The CBGX-EMS Password installation parameter defines the password for the TMF814 connection to the Navis® EMS-CBGX system. For addition information on the Navis® EMS-CBGX system, refer to the "Install the NAVIS® EMS-CBGX System" (p. 4-16) task and the "OMS_NE license" (p. 5-10) (OMS_NE_CBG).

The default value for this parameter is mountaindew.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 14.

This parameter does not require any system restart (**None**) for the parameter values to take effect. Changes take effect at the next attempt to connect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_CBGX_PASSWD.

SSH Authentication Algorithm

The SSH Authentication Algorithm installation parameter sets the encryption algorithm that is to be used by the SSH interface to the 1695 Wavelength Services Manager (WSM) NEs.

Valid values for this parameter are RSA or DSA.

The default value is RSA.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 15.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SSH_AUTH.

Drop Communication to NE for new controller card

The Drop Communication to NE for new controller card installation parameter will drop communication link to NE when the parameter detects new controller cards and is set to YES.

Valid values for this parameter are YES and NO.

The default value is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 16.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as CMISE_DROP_COMMS_ON_NEW_CTL_CARD.

Validate total NE count for CMISE Network Adaptor

The Validate total NE count for CMISE Network Adaptor installation parameter checks the maximum number of NEs allowed in a CMISE Network Adaptor.

Valid values for this parameter are Enable and Disable.

The default value is DISABLE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 17.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.CHK_NE_COUNT_CNA.

Validate total NE count for TL1 Network Adaptor

The Validate total NE count for TL1 Network Adaptor installation parameter checks the maximum number of NEs allowed in a TL1 Network Adaptor.

Valid values for this parameter are Enable and Disable.

The default value is DISABLE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 18.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.CHK_NE_COUNT_TNA.

Total NE count for CMISE Network Adaptor

The Total NE count for CMISE Network Adaptor installation parameter validates the for the maximum number of NEs allowed in a CMISE Network Adaptor.

Valid values for this parameter are [1–99999].

The default value is 400.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 19.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.NE_HARDLIMIT_CNA.

Total NE count for TL1 Network Adaptor

The Total NE count for TL1 Network Adaptor installation parameter validates the for the maximum number of NEs allowed in a TL1 Network Adaptor.

Valid values for this parameter are [1–99999].

The default value is 1000.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 20.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.NE_HARDLIMIT_TNA.

Total NE count percentage for CMISE Network Adaptor

The percentage for total NE count for CMISE Network Adaptor installation parameter provides the percentage of total NEs in a CMISE Network adaptor.

Valid values for this parameter are [1–99].

The default value is 95.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 21.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.NE_SOFTLIMIT_PERCENT_CNA.

Total NE count percentage for TL1 Network Adaptor

The percentage for total NE count for TL1 Network Adaptor installation parameter provides the percentage of total NEs in a TL1 Network adaptor.

Valid values for this parameter are [1–99].

The default value is 95.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 22.

When specifying option 17, **Display Current Values**, this installation parameter appears as EA.NE_SOFTLIMIT_PERCENT_TNA.

Time Synchronization Service

The Time Synchronization Service installation parameter enables or disables time synchronization service in NM. A adaptor for North America NEs. This parameter is only used in classic OMS.

Valid values for this parameter are YES or NO.

The default value is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 23.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as USE_TIMESYNC_SERVICE.

Time Synchronization Offset

The Time Synchronization Offset installation parameter sets the offset in seconds for the time synchronization of North American NEs. This parameter is only used in classic OMS.

Valid values for this parameter are 1 to 60 seconds.

The default value is 30 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 24.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIMESYNC_OFFSET.

Time Synchronization Polling Period

The Time Synchronization Polling Period installation parameter sets the polling period in minutes for the time synchronization of North American NEs. A value of 0 disables the polling. This parameter is only used in classic OMS.

Valid values for this parameter are 0 to 1440 minutes.

The default value is 1440 minutes.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 25.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIMESYNC_POLLING_FREQ_IN_MINUTES.

Hide In Domain

The Hide In Domain installation parameter specify whether the 'in the domain' radio button option should be displayed for black box nodes.

Valid values for this parameter are YES or NO. If the value is set to YES, the 'in the domain' radio button will not be displayed for black box nodes.

The default value is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Element Administration Variables** option, which is option 3, number 26.

This parameter does not require any system restart (**None**) for the parameter values to take effect. This parameter requires the network adapter (NA) to be restarted for the parameter values to take effect. Changes take effect at the next attempt to connect to the NE.

When specifying option 17, **Display Current Values**, this installation parameter appears as HIDE_IN_DOMAIN.

Connection Variables

Connection Name Format

The Connection Name Format installation parameter specifies the format to be displayed as the default when the user is creating a connection. The user can select the format that is being displayed or the user can select another format.

Valid values for this parameter are TELCORDIA, M1400, or FREE_FORMAT. The default Connection Name Format is TELCORDIA.

Important! For installations with the TMF814 Northbound Interface, the Connection Name Format installation parameter must be set to FREE_FORMAT, which is the default. See "TMF814 Northbound Interface installation parameters" (p. 18-7) for additional details on installation parameters and the TMF814 Northbound Interface. Other related installation parameters are "Auto Discovery Connection Name Format" (p. 6-42) and "Connection Name Separator" (p. 6-43).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CONNECTION_NAME_FORMAT.

Auto Discovery Connection Name Format

The Auto Discovery Connection Name Format installation parameter specifies the name format that the management system is to use if the "Connection Name Format" (p. 6-42) installation parameter is set to FREE_FORMAT and the system creates a connection name during an event such as Connection Auto Discovery. (Refer to Chapter 22, "Connection Auto Discovery" for details.)

Valid values for this parameter are TELCORDIA and M1400. The default is TELCORDIA.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTO_CONN_NAME_FORMAT.

Connection Name Separator

The Connection Name Separator installation parameter specifies the separator that is to be used for connection name components. Changes are not retrospectively applied to the database—existing connection names are not affected.

Valid values for this parameter are the following:

| / - _ . :

These symbols represent a pipe, forward slash, hyphen, underscore, period, colon, or a blank space.

The default is **/**, which is a forward slash.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CONNECTION_NAME_SEPARATOR.

Connection Alias

The Connection Alias installation parameter enables the operator to specify whether a connection alias that is different than the connection name should be enabled.

Valid values for this parameter are ON to enable the alias or OFF to disable the alias. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CONNECTION_ALIAS.

Connection Scheduling

The Connection Scheduling installation parameter specifies that connection scheduling (one time) is supported.

Valid values for this parameter are OFF or ONE_TIME_SCHEDULE. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CONNECTION_SCHEDULING.

Quality of Service

The Quality of Service installation parameter specifies that the quality-of-service (QoS) field on the Orders Parameters panel of connection provisioning is to be enabled.

Valid values for this parameter are ON, meaning the page is to be displayed or OFF, meaning the page is not to be displayed. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.QUALITY_OF_SERVICE.

Customer Priority

The Customer Priority installation parameter specifies that the customer priority field on the Orders parameters page of connection provisioning is to be enabled.

Valid values for this parameter are ON, meaning the page is to be displayed or OFF, meaning the page is not to be displayed. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 7.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CUSTOMER_PRIORITY.

Disable Alarms During Provisioning

The Disable Alarms During Provisioning installation parameter specifies whether the monitoring of alarms should be disabled during provisioning.

Valid values for this parameter are ON or OFF. The default is ON, which means that the monitoring of alarms is disabled during provisioning.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 8.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.DISABLE_ALARM _DURING_PROV.

CTP Alarm Monitoring

The CTP Alarm Monitoring installation parameter controls whether all termination points (TPs) on a connection, which are connection termination points (CTPs), are monitored or only the edge points are monitored. Monitoring only the edge points reduces the alarm process load on the system.

Valid values for this parameter are EDGE_ONLY or ALL. The default is EDGE_ONLY, which monitors only the edge points.

Important! For installations with the TMF814 Northbound Interface, the CTP Alarm Monitoring installation parameter must be set to ALL. See "TMF814 Northbound Interface installation parameters" (p. 18-7) for additional details on installation parameters and the TMF814 Northbound Interface.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 9.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CTP_MONITORING.

Orphan Cross Connection Deletion Tool

The Orphan Cross Connection Deletion Tool installation parameter enables the automatic execution of the cross connection deletion tool. This tool runs daily to delete cross connections that have been tagged as not required following a partial failure of a connection creation or a deletion. See "TMF814 Northbound Interface Concepts" (p. 18-2) more information about the TMF814 NBI. See the "Table of scheduled activities" (p. 41-4) for details regarding the **nwc_delete_orphan_xc** cron job.

Valid values for this parameter are YES to enable the running of the tool or NO to disable the running of the tool. The default is NO, which disables the running of the tool.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables** , which is option 4, number 10.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CROSS_CONNECT_DELETE_TOOL.

ONNS Paths Auto Retrieval

The ONNS Paths Auto Retrieval installation parameter enables the daily retrieval of Optical Network Navigator System (ONNS) paths to synchronize the OMS database with the detailed ONNS path data.

Valid values for this parameter are YES to enable the daily retrieval and synchronization or NO to disable daily retrieval and synchronization. The default is NO, which disables daily retrieval and synchronization.

Important! If you plan to run the Network Inventory Extraction Tool (see Chapter 23, “Network Inventory Extraction”), set the value for ONNS Paths Auto Retrieval installation parameter to YES.

If you want to run the ONNS Paths Auto Retrieval tool automatically, set the value for the ONNS Paths Auto Retrieval installation parameter to YES. If you want to run the ONNS Paths Auto Retrieval tool manually, set the value of this parameter to NO. See “Discover ONNS Paths Tool Concepts” (p. 34-3) for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **Connection Variables**, which is option 4, number 11.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ONNS_AUTO_RETRIEVE.

ONNS Network Type

The ONNS Network Type installation parameter indicates whether a pure controlled Optical Network Navigator System (ONNS) domain or mixed ONNS domain is supported.

Valid values for this parameter are PURE and MIXED. The default is PURE, which is a pure controlled ONNS domain.

Note: For 1675 Lambda Unite MultiService Switch (MSS) ONNS, the default parameter value is set to PURE. MIXED supports WSM NEs only.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 12.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ONNS_NETWORK_TYPE.

SNC Fail Policy

The SNC Fail Policy installation parameter specifies whether the management system should attempt to back out the partial subnetwork controller (SNC) when an SNC creation fails.

Valid values for this parameter are NO_BACKOUT_ON_FAILURE or BACKOUT_ON_FAILURE.

The default is NO_BACKOUT_ON_FAILURE, which specifies that the management system should not attempt to back out the partial SNC when an SNC creation fails.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 13.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as BACKOUT_PARTIAL_SNC_POLICY.

Show End Port Columns on Connection List

The Show End Port Columns on Connection List installation parameter specifies whether four additional columns should be displayed on the connection list for connection end ports.

Valid values for this parameter are YES or NO.

The default is NO, which specifies that four additional columns should not be displayed. Note that displaying the four additional columns adds a delay to the display response.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Connection Variables**, which is option 4, number 14.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as CONN_LIST_COLS.

Enable Port User Label

The Enable Port User Label installation parameter specifies whether the user label field that is associated with ports is enabled or disabled.

Valid values for this parameter are YES, which enables the field, and No, which disables the field. The default is No, which disables the field. When this installation parameter is set to Yes, all appropriate GUI pages/screens display the User Label for Ports field. Refer to the *OMS Network Element Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 15.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PORT_USER_LABEL.

Allow Delete, Convert, and Rollback on Correlated Cross Connects

The Allow Delete, Convert, and Rollback on Correlated Cross Connects installation parameter specifies whether a correlated cross connect can be deleted, converted, or rolled back.

Valid values for this parameter are YES, which enables the field, and NO, which disables the field. The default is NO, which disables the field. When this installation parameter is set to Yes, a correlated cross connect can be deleted, converted, or rolled back.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 16.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ALLOW_CORREL_XC_DELETE.

CTP Address Format for Non-managed NEs

The CTP Address Format for Non-managed NEs installation parameter specifies the format in which the non-managed NE CTP nativename is generated.

Valid values for this parameter are G707 or SEQUENTIAL. The default is G707.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 17.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NNE_CTP_ADDRESS_FORMAT.

Enable ASAP Fields on Provisioning Panel

The Enable ASAP Fields on Provisioning Panel installation parameter specifies whether the alarm severity assignment profile (ASAP) fields should be enabled on the Connections provisioning panel.

Valid values for this parameter are ENABLED and DISABLED. The default is DISABLED.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 18.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ASAP_PROVISIONING.

Enable Display of Service State on Graphical Layout

The Enable Display of Service State on Graphical Layout installation parameter enables the display of the service state on the graphical layout.

Valid values for this parameter are YES and NO. The default is NO, which disables the display of the service state.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 19.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SERVICE_STATE_SUPPORT.

Retain Black Box Cross Connections

The Retain Black Box Cross connections installation parameter specifies whether a black box cross connection retention is enabled when network connection passing through black box is dbdeleted.

Valid values for this parameter are YES, meaning the black box cross connection retention is enabled or NO, meaning that the black box cross connection retention is NOT enabled. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 20.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as RETAIN_BBOX_XCS_WHEN_NC_DBDELETED.

Enable display of LTU ports

The Enable display of LTU ports installation parameter enables display of LTU ports when set to YES.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 21.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ALLOW_LTU_CTPS.

Enable display of Protection Switch Status-Automatic

The Enable display of Protection Switch Status-Automatic installation parameter enables the display of protection switch status to Automatic mode when set to YES.

Valid values for this parameter are YES or NO. The default is YES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 22.

When specifying option 17, **Display Current Values**, this installation parameter appears as DISPLAY_PSW_AUTO.

Enable display of Protection Switch Status-Selectable

The Enable display of Protection Switch Status-Selectable installation parameter enables the display of protection switch status to Selectable modewhen set to YES.

Valid values for this parameter are YES or NO. The default is YES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 23.

When specifying option 17, **Display Current Values**, this installation parameter appears as DISPLAY_PSW_SELECT.

Enable display of XC Loopbacks

The Enable display of XC Loopbacks installation parameter displays the enhanced cross connection loopback menu of the Graphical Layout when set to YES. The enhanced cross connection loopback menu allows a user to operate/release a cross connection loopback from the Graphical Layout.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 24.

When specifying option 17, **Display Current Values**, this installation parameter appears as DISPLAY_XC_LOOPBACK.

Enable triggering Network Connection

The Enable triggering Network Connection installation parameter enables the triggering of network connection upon notification or SNC sync.

Valid values for this parameter are YES or NO. The default is YES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 25.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.CORRELATE_SNC_TRIG.

Modify Route of an Inconsistent Connection

The Modify Route of an Inconsistent Connection installation parameter determines if modify route is supported for an inconsistent connection. A value of "BLOCK" means that all requests to modify the route of an Inconsistent Connections will be blocked including both hard and soft rearrange.

Valid values for this parameter are ALLOW or BLOCK. The default is BLOCK.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Connection Variables** option, which is option 4, number 26.

When specifying option 17, **Display Current Values**, this installation parameter appears as NWC.MODIFY_INCONSISTENT_CONN.

Ethernet Variables

Default Option for Spoke Level 2 Switching

The Default Option for Spoke Level 2 Switching installation parameter specifies the default value for Ethernet spoke layer 2 switching on the Additional Spoke Parameters page of the management system.

Valid values for this parameter are SWITCHED or NONSWITCHED. The default is NONSWITCHED.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Ethernet Variables**, which is option 5, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as EM_SPOKE_SWITCHING_DEFAULT.

Enable Automatic Deletion Of Empty VCGs

The Enable Automatic Deletion Of Empty VCGs installation parameter specifies whether the automatic deletion of empty VCGs should be enabled or disabled.

Valid values for this parameter are YES or NO. The default is NO, which disables the option.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Ethernet Variables**, which is option 5, number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits.

When specifying option 17, **Display Current Values**, this installation parameter appears as EM_AUTO_DELETE_EMPTY_VCG.

Order Handling Variables

Order Versioning

The Order Versioning installation parameter specifies whether or not the order version is shown and whether or not can be edited.

Valid values for this parameter are ON or OFF. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.ORDER_VERSIONING.

History Order Storage Time

The History Order Storage Time installation parameter specifies the time, in hours, for which the history order is to be retained.

Valid values for this parameter are 0 hours to 168 hours, which is 1 week. The default is 0 hours.

Important! For installations with High Availability, the History Order Storage Time installation parameter must be set to 24 hours. See "TMF814 Northbound Interface installation parameters" (p. 18-7) for additional details on installation parameters and the TMF814 Northbound Interface.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 2.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.KEEP_HISTORY_ORDER.

Reuse Order Number

The Reuse Order Number installation parameter specifies whether an order number can be reused for active objects.

Valid values for this parameter are OFF, meaning the order number cannot be reused for active objects or MODIFY, meaning that the modification of an object can reuse the same order number. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as REUSE_ORDER_NUMBER.

Retention Period for Failed Requests

For requests that are originated by the Ethernet Management Element Level Management (EML) only, the Retention Period for Failed Requests installation parameter specifies the value in hours in which the management system must retain failed order requests.

Valid values for this parameter are 0 hours to 168 hours, which is 7 days. The default is 24 hours.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.KEEP_FAILED_REQUESTS.

Enable Deletion of Rearrange with Reinstate History Orders

The Enable Deletion of Rearrange with Reinstate History Orders installation parameter enables the system to purge the Rearrange with Reinstate (RR) history orders automatically.

Valid values for this parameter are YES and NO. The default is NO, which does not enable the automatic deletion of the Rearrange with Reinstate (RR) history orders. If this parameter is set to YES, refer to the "Rearrange with Reinstate History Order Storage Time (Hours)" (p. 6-57) installation parameter for additional parameter settings that must be made.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.ENABLE_RR_HIS_ORDER_PURGE.

Rearrange with Reinstate History Order Storage Time (Hours)

The Rearrange with Reinstate History Order Storage Time (Hours) installation parameter defines the length of time in hours for which rearrange with reinstate history orders are retained if the "Enable Deletion of Rearrange with Reinstate History Orders" (p. 6-56) installation parameter set to YES.

Valid values for this parameter are 0 hours to 168 hours, which is 1 week. The default is 0 hours.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.KEEP_HISTORY_ORDER_RR.

Default Stop Step

The Default Stop Step installation parameter defines the default for the order step control field on the GUI for add and rearrange orders.

Valid values for this parameter are INEFFECT, PLANNED, LOCALDESIGN, or IMPLEMENTATION. Note that the value LOCALDESIGN displays behavior that is equivalent to that of WS-NMS.

The default is INEFFECT.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 7.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.DEFAULT_STOP_STEP.

Default Preplan Restoration Stop Step

The Default Preplan Restoration Stop Step installation parameter defines the default for the order step control field on the GUI for preplan restoration orders.

Valid values for this parameter are PLANNED, LOCALDESIGN, or PREPLANCOMPLETE.

The default is PREPLANCOMPLETE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Order Handling Variables**, which is option 6, number 8.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OH.DEFAULT_PREPLAN_STOP_STEP.

PM Variables - Threshold Options

PM 24 Hour Retention Threshold

The PM 24 Hour Retention Threshold installation parameter specifies the period in days for which the system is to retain 24-hour performance data. When the threshold specified is exceeded, the data is deleted. In addition, the data is deleted if the storage size limit is reached within the retention period.

Valid values for this parameter are 1 to 62 days. The default is 31 days.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_24H_THRESHOLD.

PM 15 Minute Retention Threshold

The PM 15 Minute Retention Threshold installation parameter specifies the period in days for which the system is to retain 15 minute performance data. When the threshold specified is exceeded, the data is deleted. In addition, the data is deleted if the storage size limit is reached within the retention period.

Valid values for this parameter are 1 to 28 days. The default is 1 day.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, number 2.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_15M_THRESHOLD.

PM Variables - PM Panel Settings - Network Connections

15 Minute Monitor Type (for Network Connections)

The 15 Minute Monitor Type (for Network Connections) installation parameter specifies the default 15 minute performance monitoring type for provisioning network connections.

Valid values for this parameter are ALL, END_XCS, PROTECTION, or NONE. The default is NONE. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 3, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_NC.

15 Minute Collect/Monitor (for Network Connections)

The 15 Minute Collect/Monitor (for Network Connections) installation parameter specifies the action the management system is to take regarding the 15-minute network connections (NC) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 3, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_NC.

15 Minute Interval (for Network Connections)

The 15 Minute Interval (for Network Connections) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for network connections is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_NC.

24 Hour Monitor Type (for Network Connections)

The 24-Hour Monitor Type (for Network Connections) installation parameter specifies the default 24 hour performance monitoring type for provisioning network connections.

Valid values for this parameter are ALL, END_XCS, PROTECTION, or NONE. The default is NONE. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_NC.

24 Hour Collect/Monitor (for Network Connections)

The 24 Hour Collect/Monitor (for Network Connections) installation parameter specifies the action the management system is to take regarding the 24-hour network connections (NC) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_NC.

24 Hour Interval (for Network Connections)

The PM_PANEL_24H_INT_NC installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for network connections is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_NC.

Bi-Directional 24 Hour Monitor Type (for Network Connections)

The Bi-Directional 24-Hour Monitor Type (for Network Connections) installation parameter specifies the default bi-directional 24 hour performance monitoring type for provisioning network connections.

Valid values for this parameter are ALL, END_XCS, PROTECTION, or NONE. The default is NONE. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 7.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_MON_NC.

Bi-Directional 24 Hour Collect/Monitor (for Network Connections)

The Bi-Directional 24 Hour Collect/Monitor (for Network Connections) installation parameter specifies the action the management system is to take regarding the 24-hour network connections (NC) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 8.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_COLL_NC.

Bi-Directional 24 Hour Interval (for Network Connections)

The Bi-Directional 24 Hour Interval (for Network Connections) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for network connections is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning network connections, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, then select number 3, then number 9.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_INT_NC.

PM Variables - PM Panel Settings - VCGs

15 Minute Monitor Type (for VCGs)

The 15 Minute Monitor Type (for VCGs) installation parameter specifies the default 15 minute performance monitoring type for provisioning virtual concatenation groups (VCGs).

Valid values for this parameter are END_XCS and NONE. The default is NONE. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_VCG.

15 Minute Collect/Monitor (for VCGs)

The PM_PANEL_15M_COLL_VCG installation parameter specifies the action the management system is to take regarding the 15-minute virtual concatenation group (VCG) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_VCG.

15 Minute Interval (for VCGs)

The 15 Minute Interval (for VCGs) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for virtual concatenation groups (VCGs) is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_VCG.

24 Hour Monitor Type (for VCGs)

The 24 Hour Monitor Type (for VCGs) installation parameter specifies the default 24 hour performance monitoring type for provisioning virtual concatenation groups (VCGs).

Valid values for this parameter are END_XCS and NONE. The default is NONE. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_VCG.

24 Hour Collect/Monitor (for VCGs)

The 24 Hour Collect/Monitor (for VCGs) installation parameter specifies the action the management system is to take regarding the 24-hour virtual concatenation group (VCG) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_VCG.

24 Hour Interval (for VCGs)

The 24 Hour Interval (for VCGs) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for virtual concatenation groups (VCGs) is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A a value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_VCG.

Bi-Directional 24 Hour Monitor Type (for VCGs)

The Bi-Directional 24 Hour Monitor Type (for VCGs) installation parameter specifies the default 24 hour performance monitoring type for provisioning virtual concatenation groups (VCGs).

Valid values for this parameter are END_XCS and NONE. The default is NONE. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 7.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_MON_VCG.

Bi-Directional 24 Hour Collect/Monitor (for VCGs)

The Bi-Directional 24 Hour Collect/Monitor (for VCGs) installation parameter specifies the action the management system is to take regarding the 24-hour virtual concatenation group (VCG) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 8.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_COLL_VCG.

Bi-Directional 24 Hour Interval (for VCGs)

The Bi-Directional 24 Hour Interval (for VCGs) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for virtual concatenation groups (VCGs) is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A a value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning VCGs, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 4, then number 9.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_BI_24H_INT_VCG.

PM Variables - PM Panel Settings - Ethernet Non Switched Service

15 Minute Monitor Type (for Ethernet Non Switched Service)

The 15 Minute Monitor Type (for Ethernet Non Switched Service) installation parameter specifies the default 15 minute performance monitoring type for provisioning Ethernet Non-Switched services.

Valid values for this parameter are ALL, END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_NON.

15 Minute Collect/Monitor (for Ethernet Non Switched Service)

The 15 Minute Collect/Monitor (for Ethernet Non Switched Service) installation parameter specifies the action the management system is to take regarding the 15-minute Ethernet Non-Switched services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_NS.

15 Minute Interval (for Ethernet Non Switched Service)

The 15 Minute Interval (for Ethernet Non Switched Service) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for Ethernet Non-Switched services is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_NS.

24 Hour Monitor Type (for Ethernet Non Switched Service)

The 24 Hour Monitor Type (for Ethernet Non Switched Service) installation parameter specifies the default 24 hour performance monitoring type for provisioning Ethernet Non-Switched services.

Valid values for this parameter are ALL, END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_NON.

24 Hour Collect/Monitor (for Ethernet Non Switched Service)

The 24 Hour Collect/Monitor (for Ethernet Non Switched Service) installation parameter specifies the action the management system is to take regarding 24-hour Ethernet Non-Switched services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_NS.

24 Hour Interval (for Ethernet Non Switched Service)

The 24 Hour Interval (for Ethernet Non Switched Service) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for Ethernet Non-Switched services is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning Ethernet Non-Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 5, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_NS.

PM Variables - PM Panel Settings - Ethernet Switched Service

15 Minute Monitor Type (for Ethernet Switched Service)

The 15 Minute Monitor Type (for Ethernet Switched Service) installation parameter specifies the default 15 minute performance monitoring type for provisioning Ethernet Switched services.

Valid values for this parameter are END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 6, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_SW.

15 Minute Collect/Monitor (for Ethernet Switched Service)

The 15 Minute Collect/Monitor (for Ethernet Switched Service) installation parameter specifies the action the management system is to take regarding the 15-minute Ethernet Switched services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 6, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_SW.

15 Minute Interval (for Ethernet Switched Service)

The 15 Minute Interval (for Ethernet Switched Service) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for Ethernet Switched services is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables**, which is option 7; then select number 6, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_SW.

24 Hour Monitor Type (for Ethernet Switched Service)

The 24 Hour Monitor Type (for Ethernet Switched Service) installation parameter specifies the default 24 hour performance monitoring type for provisioning Ethernet Switched services.

Valid values for this parameter are END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 6, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_SW.

24 Hour Collect/Monitor (for Ethernet Switched Service)

The 24 Hour Collect/Monitor (for Ethernet Switched Service) installation parameter specifies the action the management system is to take regarding the 24-hour Ethernet Switched services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 6, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_SW.

24 Hour Interval (for Ethernet Switched Service)

The 24 Hour Interval (for Ethernet Switched Service) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for Ethernet Switched services is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning Ethernet Switched services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 6, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_SW.

PM Variables - PM Panel Settings - Hub & Spoke Service

15 Minute Monitor Type (for Hub & Spoke Service)

The 15 Minute Monitor Type (for Hub & Spoke Service) installation parameter specifies the default 15 minute performance monitoring type for provisioning Ethernet Hub-and-Spoke services.

Valid values for this parameter are ALL, END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_HS.

15 Minute Collect/Monitor (for Hub & Spoke Service)

The 15 Minute Collect/Monitor (for Hub & Spoke Service) installation parameter specifies the action the management system is to take regarding the 15-minute Ethernet Hub-and-Spoke services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_HS.

15 Minute Interval (for Hub & Spoke Service)

The 15 Minute Interval (for Hub & Spoke Service) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for Ethernet Hub-and-Spoke services is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_HS.

24 Hour Monitor Type (for Hub & Spoke Service)

The 24 Hour Monitor Type (for Hub & Spoke Service) installation parameter specifies the default 24 hour performance monitoring type for provisioning Ethernet Hub-and-Spoke services.

Valid values for this parameter are ALL, END_PORTS, and NONE. The default is NONE. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_HS.

24 Hour Collect/Monitor (for Hub & Spoke Service)

The 24 Hour Collect/Monitor (for Hub & Spoke Service) installation parameter specifies the action the management system is to take regarding the 24-hour Ethernet Hub-and-Spoke services data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_HS.

24 Hour Interval (for Hub & Spoke Service)

The 24 Hour Interval (for Hub & Spoke Service) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for Ethernet Hub-and-Spoke services is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A a value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning Ethernet Hub-and-Spoke services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 7, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_HS.

PM Variables - PM Panel Settings - Virtual Switch Network

15 Minute Monitor Type (for Virtual Switch Network)

The 15 Minute Monitor Type (for Virtual Switch Network) installation parameter specifies the default 15 minute performance monitoring type for provisioning Ethernet Virtual Switch Network (VSN) services.

Valid values for this parameter are ALL and NONE. The default is NONE. When provisioning Ethernet Virtual Switch Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_VSN.

15 Minute Collect/Monitor (for Virtual Switch Network)

The 15 Minute Collect/Monitor (for Virtual Switch Network) installation parameter specifies the action the management system is to take regarding the 15-minute Ethernet Virtual Switch Network (VSN) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Virtual Switch Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_VSN.

15 Minute Interval (for Virtual Switch Network)

The 15 Minute Interval (for Virtual Switch Network) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for Ethernet Virtual Switch Networks (VSNs) is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning Ethernet Virtual Switch Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_VSN.

24 Hour Monitor Type (for Virtual Switch Network)

The 24 Hour Monitor Type (for Virtual Switch Network) installation parameter specifies the default 24 hour performance monitoring type for provisioning Ethernet Virtual Switch Network (VSN) Services.

Valid values for this parameter are ALL and NONE. The default is NONE. When provisioning Ethernet Virtual Switch Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_VSN.

24 Hour Collect/Monitor (for Virtual Switch Network)

The 24 Hour Collect/Monitor (for Virtual Switch Network) installation parameter specifies the action the management system is to take regarding the 24-hour Ethernet Virtual Switch Network (VSN) data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Ethernet Virtual Switched Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_VSN.

24 Hour Interval (for Virtual Switch Network)

The 24 Hour Interval (for Virtual Switch Network) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for Ethernet Virtual Switch Networks (VSNs) is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning Ethernet Virtual Switch Network services, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Ethernet Management Guide* for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 8, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_VSN.

PM Variables - PM Panel Settings - Control Plane Service

15 Minute Monitor Type (for Control Plane Service)

The 15 Minute Monitor Type (for Control Plane Service) installation parameter specifies the default 15 minute performance monitoring type for provisioning Control Plane Service.

Valid values for this parameter are END_PORTS and NONE. The default is NONE. When provisioning Control Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_MON_ASTN.

15 Minute Collect/Monitor (for Control Plane Service)

The 15 Minute Collect/Monitor (for Control Plane Service) installation parameter specifies the action the management system is to take regarding the 15-minute Control Plane Service data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Control

Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_COLL_ASTN.

15 Minute Interval (for Control Plane Service)

The 15 Minute Interval (for Control Plane Service) installation parameter specifies the interval, in minutes, for which 15-minute performance monitoring data for Control Plane Service is to be monitored or collected.

Valid values for this parameter are 0 minutes through 480 minutes, which is 8 hours. The default is 60 minutes. Any value specified is rounded up to the nearest 15-minute interval. When provisioning Control Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_15M_INT_ASTN.

24 Hour Monitor Type (for Control Plane Service)

The 24 Hour Monitor Type (for Control Plane Service) installation parameter specifies the default 24 hour performance monitoring type for provisioning Control Plane Service.

Valid values for this parameter are END_PORTS and NONE. The default is NONE. When provisioning Control Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_MON_ASTN.

24 Hour Collect/Monitor (for Control Plane Service)

The 24 Hour Collect/Monitor (for Control Plane Service) installation parameter specifies the action the management system is to take regarding the 24-hour Control Plane Service data.

Valid values for this parameter are COLLECT, in which the management system collects the data, or MONITOR, in which the data is stored on the NE and the management system simply monitors the data. The default is COLLECT. When provisioning Control Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_COLL_ASTN.

24 Hour Interval (for Control Plane Service)

The 24 Hour Interval (for Control Plane Service) installation parameter specifies the interval, in days, for which 24-hour performance monitoring data for PM Control Plane Service is to be monitored or collected.

Valid values for this parameter are 0 days through 7 days. The default is 1 day. A value of 0 days indicates that the monitoring or collection is not automatically stopped. When provisioning Control Plane Service, users can override the setting for this installation parameter by modifying the value that is displayed in the Assurance parameters panel. Refer to the *OMS Connection Management Guide* for provisioning details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7; then select number 9, then number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_PANEL_24H_INT_ASTN.

PM Variables - PM Panel UNI/BI Best Effort

PM Panel UNI/BI Best Effort

The PM Panel UNI/BI Best Effort installation parameter specifies whether bidirectional (BI) and non-bidirectional (UNI) fields should be displayed and managed separately in the Assurance Panel of the management system.

Valid values for this parameter are DISABLED or ENABLED. The default is DISABLED, which results in the UNI and BI fields being displayed and managed separately in the Assurance Panel of the management system. When ENABLED, one 24-hour option is displayed—the management system enables the 24-hour BI if the NE supports 24-hour BI or the 24-hour UNI if the NE does not support 24-hour BI.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **Performance Management Variables** option, which is option 7, number 10.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PM_BEST_EFFORT.

System Variables

Date Format

The Date Format installation parameter specifies a format for the date of the year.

Valid values for this parameter are DD/MM/YY, DD/MM/YY, YY/MM/DD, MM/DD/YYYY, DD/MM/YYYY, and YYYY/MM/DD. The default is DD/MM/YY.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DATE_FORMAT.

Time Format

The Time Format installation parameter specifies the format for the time of the day.

Valid values for this parameter are 23:59:00. The default is 23:59:00.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIME_FORMAT.

Time Zone

The Time Zone installation parameter specifies the initial current time zone that the management system is to use for its users. (This parameter does not affect overall system housekeeping functions, which are set from the server.)

Valid values for this parameter are a list of over 25 values that are extracted from the Java libraries; for example: MIT, Pacific/Tahiti, America/Phoenix.... The default is GMT+00:00.

For considerations involving Data Extraction, refer to "Data Extraction report time zone" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 3.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIME_ZONE.

Map Background

The Map Background installation parameter identifies the background of the Network Map display.

The valid value for this parameter is the list of backgrounds that can be used. The default is *world*.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as MAP_BACKGROUND.

Default Terminology (SONET/SDH)

The Default Terminology (SONET/SDH) installation parameter specifies whether the management system terminology should be SONET or SDH.

If the "Terminology Choice" (p. 6-90) installation parameter is set to ON, the setting of this installation parameter is overridden when users select either SONET or SDH in the **Application Preferences** setting on the **Preferences** page in the management system. See the *OMS Getting Started Guide* for instructions on how to change preferences.

If the "Terminology Choice" (p. 6-90) installation parameter is set to OFF, the terminology is fixed to the value selected using the Default Terminology installation parameter.

Valid values for this parameter are SONET or SDH. The default is SONET.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SYS.TERMINOLOGY.

Enable ONNS Feature

The Enable ONNS Feature installation parameter, which is only applicable for special installations in the SDH and SONET environment, specifies whether support for the Optical Network Navigator System (ONNS) should be enabled or disabled. See the "Connection Management user task" (p. 7-9) for interworking implications.

Valid values for this parameter are ON to enable ONNS support or OFF to disable ONNS support. The default is OFF to disable ONNS support.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 6.

A related platform alarm is "ONNS_ASSOC_LOST" (p. 42-22).

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SYS.ONNS_ENABLED.

Default TP Name to Show

The Default TP Name to Show installation parameter specifies whether a management system displays to the user the termination point native name (TPNativeName) or the termination point relative time slot name (TPRelativeTimeslotName).

Valid values for this parameter are TPNativeName or TPRTSName. The default is TPNativeName.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SYS.DEFAULT_TP_NAME.

Terminology Choice

The Terminology Choice installation parameter specifies whether the choice afforded by the Terminology radio button that appears in the Application preferences portion of the management system **Preferences** page should be suppressed.

Valid values for this parameter are OFF and ON. The default is OFF, which suppresses the Terminology radio button; hence the terminology is fixed to the value selected using the "Default Terminology (SONET/SDH)" (p. 6-89) installation parameter.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 8.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SYS.TERM_CONTROL.

Scheduled Job Restart

The Scheduled Job Restart installation parameter sets the processing policy for scheduled activities after a restart.

Valid values for this parameter are RUN_OVERDUE, in which all overdue tasks are processed upon a restart, or DROP_OVERDUE, in which all overdue tasks are not run. The default is RUN_OVERDUE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 9.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SCHEDULED_JOB_RESTART.

OV Server

Valid values for this parameter are TRUE and FALSE.

The default value is FALSE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **System Variables**, which is option 8, number 10.

When specifying option 17, **Display Current Values**, this installation parameter appears as A_OV.

Data Extraction Variables for NE Report

Enable NE Report in Push/Pull Mode

The Enable NE Report in Push/Pull Mode installation parameter specifies whether the NE data report is to be created and transferred to a remote system.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_NE_DATA.

NE Report Retention Period

The NE Report Retention Period installation parameter specifies the data retention period, in days, for NE data.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NE_DATA_RETENTION.

Remote Machine IP for Push Mode NE Report

The Remote Machine IP for Push Mode NE Report installation parameter specifies the IP address of the remote machine for the NE report to be transferred to when the NE report is configured in PUSH mode.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NE_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode NE Report

The Remote Machine Login ID for Push Mode NE Report installation parameter specifies a valid **ftp** login on the remote machine for the NE report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NE_REMOTE_LOGIN.

Remote Machine Password for Push Mode NE Report

The Remote Machine Password for Push Mode NE Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode NE Report (DET.NE_REMOTE_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NE_REMOTE_PASSWORD.

Remote Directory Name for Push Mode NE Report

The Remote Directory Name for Push Mode NE Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode NE Report (DET.NE_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "NE Data Files" (p. 16-21).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for NE Report, which is option 2; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NE_REMOTE_DIRECTORY.

Data Extraction Variables for Equipment Report

Enable Equipment Report in Push/Pull Mode

The Enable Equipment Report in Push/Pull Mode installation parameter specifies whether the equipment report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Equipment Data Files" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_EQPT_DATA.

Equipment Report Retention Period (Days)

The Equipment Report Retention Period installation parameter specifies the data retention period, in days, for the equipment report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "Equipment Data Files" (p. 16-8)T.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.EQPT_DATA_RETENTION.

Remote Machine IP for Push Mode Equipment Report

The Remote Machine IP for Push Mode Equipment Report installation parameter specifies the IP address of the remote machine for the Equipment Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "Equipment Data Files" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.EQUIP_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode Equipment Report

The Remote Machine Login ID for Push Mode Equipment Report installation parameter specifies a valid **ftp** login on the remote machine for the Equipment Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to "Equipment Data Files" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.EQUIP_REMOTE_LOGIN.

Remote Machine Password for Push Mode Equipment Report

The Remote Machine Password for Push Mode Equipment Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode Equipment Report (DET.EQUIP_REMOTE_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to "Equipment Data Files" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.EQUIP_REMOTE_PASSWORD.

Remote Directory Name for Push Mode Equipment Report

The Remote Directory Name for Push Mode Equipment Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode Equipment Report (DET.EQUIP_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "Equipment Data Files" (p. 16-8).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Equipment Report, which is option 3; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.EQUIP_REMOTE_DIRECTORY.

Data Extraction Variables for All Alarm Report

Enable All Alarm Report in Push/Pull Mode

The Enable All Alarm Report in Push/Pull Mode installation parameter specifies whether the all alarm report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_ALL_ALM_DATA.

All Alarm Report Retention Period (Days)

The All Alarm Report Retention Period installation parameter specifies the data retention period, in days, for the All Alarm report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALL_ALM_RETENTION.

Interval (Days) for All Alarm Report

The Interval for All Alarm Report installation parameter specifies the alarm interval, in days, for all alarm data.

Valid values for this parameter are 1 through any number of days that are greater than 1 day. The default is 1 day. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALL_ALM_INTERVAL.

Remote Machine IP for Push Mode All Alarm Report

The Remote Machine IP for Push Mode All Alarm Report installation parameter specifies the IP address of the remote machine for the All Alarm Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALLALM_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode All Alarm Report

The Remote Machine Login ID for Push Mode All Alarm Report installation parameter specifies a valid **ftp** login on the remote machine for the All Alarm Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALLALM_REMOTE_LOGIN.

Remote Machine Password for Push Mode All Alarm Report

The Remote Machine Password for Push Mode All Alarm Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode All Alarm Report (DET.ALLALM_REMOTE-_LOGIN) installation parameter. he stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALLALM_REMOTE_PASSWORD.

Remote Directory Name for Push Mode All Alarm Report

The Remote Directory Name for Push Mode All Alarm Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode All Alarm Report (DET.ALLALM_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "All Alarm Data Files" (p. 16-17).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for All Alarm Report, which is option 4; then select number 7.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ALLALM_REMOTE_DIRECTORY.

Data Extraction Variables for Active Alarm Report

Enable Active Alarm Report in Push/Pull Mode

The Enable Active Alarm Report in Push/Pull Mode installation parameter specifies whether the active alarm report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Active Alarm Data Files" (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_ACT_ALM_DATA.

Active Alarm Report Retention Period (Days)

The Active Alarm Report Retention Period installation parameter specifies the data retention period, in days, for the Active Alarm report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "Active Alarm Data Files" (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACT_ALM_RETENTION.

Interval (Days) for Active Alarm Report

The Interval for Active Alarm Report installation parameter specifies the alarm interval, in days, for Active Alarm data.

Valid values for this parameter are 1 through any number of days that are greater than 1 day. The default is 1 day. To receive the entire (all) Active Alarm list, specify 99999. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Active Alarm Data Files" (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACT_ALM_INTERVAL.

Remote Machine IP for Push Mode Active Alarm Report

The Remote Machine IP for Push Mode Active Alarm Report installation parameter specifies the IP address of the remote machine for the Active Alarm Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "Active Alarm Data Files" (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACTALM_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode Active Alarm Report

The Remote Machine Login ID for Push Mode Active Alarm Report installation parameter specifies a valid **ftp** login on the remote machine for the Active Alarm Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to “Active Alarm Data Files” (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACTALM_REMOTE_LOGIN.

Remote Machine Password for Push Mode Active Alarm Report

The Remote Machine Password for Push Mode Active Alarm Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode Active Alarm Report (DET.ALLALM_REMOTE_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to “Active Alarm Data Files” (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACTALM_REMOTE_PASSWORD.

Remote Directory Name for Push Mode Active Alarm Report

The Remote Directory Name for Push Mode Active Alarm Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode Active Alarm Report (DET.ALLALM_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "Active Alarm Data Files" (p. 16-19).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Active Alarm Report, which is option 5; then select number 7.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.ACTALM_REMOTE_DIRECTORY.

Data Extraction Variables for Network Connection Report

Enable Network Connection Report in Push/Pull Mode

The Enable Network Connection Report in Push/Pull Mode installation parameter specifies whether the network connection report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_NC_DATA.

Network Connection Report Retention Period (Days)

The Network Connection Report Retention Period installation parameter specifies the data retention period, in days, for network connection data.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NC_DATA_RETENTION.

Remote Machine IP for Push Mode Network Connection Report

The Remote Machine IP for Push Mode Network Connection Report installation parameter specifies the IP address of the remote machine for the Network Connection Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NC_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode Network Connection Report

The Remote Machine Login ID for Push Mode Network Connection Report installation parameter specifies a valid **ftp** login on the remote machine for the Network Connection Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NC_REMOTE_LOGIN.

Remote Machine Password for Push Mode Network Connection Report

The Remote Machine Password for Push Mode Network Connection Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode Network Connection Report (DET.NC_REMOTE_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NC_REMOTE_PASSWORD.

Remote Directory Name for Push Mode Network Connection Report

The Remote Directory Name for Push Mode Network Connection Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode Network Connection Report (DET.NC_REMOTE-_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "Network Connections Data Files" (p. 16-25).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Network Connection Report, which is option 6; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NC_REMOTE_DIRECTORY.

Data Extraction Variables for PM 24 Hour Report

Enable PM 24HR Report in Push/Pull Mode

The Enable PM 24HR Report in Push/Pull Mode installation parameter specifies whether the PM 24HR report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_PM_24HR.

PM 24HR Report Retention Period (Days)

The PM 24HR Report Retention Period installation parameter specifies the data retention period, in days, for the PM 24HR report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM_24HR_RETENTION.

Interval (Days) for PM 24HR Report

The Interval for PM 24HR Report installation parameter specifies the alarm interval, in days, for the PM 24HR report.

Valid values for this parameter are 1 through 30 days. The default is 1 day. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM_24HR_INTERVAL.

Remote Machine IP for Push Mode PM 24HR Report

The Remote Machine IP for Push Mode PM 24HR Report installation parameter specifies the IP address of the remote machine for the PM 24HR Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM24_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode PM 24HR Report

The Remote Machine Login ID for Push Mode PM 24HR Report installation parameter specifies a valid **ftp** login on the remote machine for the PM 24HR Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to “PM Data Files” (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM24_REMOTE_LOGIN.

Remote Machine Password for Push Mode PM 24HR Report

The Remote Machine Password for Push Mode PM 24HR Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode PM 24HR Report (DET.PM24_REMOTE_LOGIN) installation parameter.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to “PM Data Files” (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM24_REMOTE_PASSWORD.

Remote Directory Name for Push Mode PM 24HR Report

The Remote Directory Name for Push Mode PM 24HR Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode PM 24HR Report (DET.PM24_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 24HR Report, which is option 7; then select number 7.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM24_REMOTE_DIRECTORY.

Data Extraction Variables for PM 15 Minute Report

Enable PM 15min Report in Push/Pull Mode

The Enable PM 15min Report in Push/Pull Mode installation parameter specifies whether the PM 15min report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. PULL mode means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF, which is the default, means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_PM_15MIN.

PM 15min Report Retention Period (Days)

The PM 15min Report Retention Period installation parameter specifies the data retention period, in days, for the PM15min report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM_15MIN_RETENTION.

Interval (Hours) for PM 15min Report

The Interval for PM 15min Report installation parameter specifies the interval, in hours, for the PM 15min report.

Valid values for this parameter are 1 through 72 hours. The default is 24 hours, which is 1 day. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM_15MIN_INTERVAL.

Remote Machine IP for Push Mode PM 15min Report

The Remote Machine IP for Push Mode PM 15min Report installation parameter specifies the IP address of the remote machine for the PM 15min Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM15_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode PM 15min Report

The Remote Machine Login ID for Push Mode PM 15min Report installation parameter specifies a valid **ftp** login on the remote machine for the PM 15min Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM15_REMOTE_LOGIN.

Remote Machine Password for Push Mode PM 15min Report

The Remote Machine Password for Push Mode PM 15min Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode PM 15min Report (DET.PM15_REMOTE_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM15_REMOTE_PASSWORD.

Remote Directory Name for Push Mode PM 15min Report

The Remote Directory Name for Push Mode PM 15min Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode PM 15min Report (DET.PM15_REMOTE_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "PM Data Files" (p. 16-23).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for PM 15min Report, which is option 8; then select number 7.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.PM15_REMOTE_DIRECTORY.

Data Extraction Variables for Link Connection Report

Enable Link Connection Report in Push/Pull Mode

The Enable Link Connection Report in Push/Pull Mode installation parameter specifies whether the link connection report is to be created and transferred to a remote machine.

Valid values for this parameter are PULL, PUSH, and OFF. The default is PULL mode, which means that the report is going to be generated. PUSH mode means that the report is going to be generated and is going to be transferred via **ftp** to a remote machine automatically. OFF means that an report is not going to be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.DO_LC_DATA.

Link Connection Report Retention Period (Days)

The Link Connection Report Retention Period installation parameter specifies the data retention period, in days, for the link connection report.

Valid values for this parameter are 1 through 7 days. The default is 3 days.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.LC_DATA_RETENTION.

Remote Machine IP for Push Mode Link Connection Report

The Remote Machine IP for Push Mode Link Connection Report installation parameter specifies the IP address of the remote machine for the Link Connection Report.

A valid value for this parameter is a string in the format of xxx.xxx.xxx.xxx that represents the IP address of the remote machine.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.LC_REMOTE_MACHINE.

Remote Machine Login ID for Push Mode Link Connection Report

The Remote Machine Login ID for Push Mode Link Connection Report installation parameter specifies a valid **ftp** login on the remote machine for the Link Connection Report.

A valid value for this parameter is a string of alphanumeric characters that represents a login on the remote machine.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.LC_REMOTE_LOGIN.

Remote Machine Password for Push Mode Link Connection Report

The Remote Machine Password for Push Mode Link Connection Report installation parameter specifies the password that is to be used along with the login specified in the Remote Machine Login ID for Push Mode Link Connection Report (DET.LC_REMOTE-_LOGIN) installation parameter. The stored and displayed value of the password is encrypted.

A valid value for this parameter is a string of alphanumeric characters that represents the password for the remote machine. Any value that is specified can be overridden when Data Extraction is executed from the command line.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.LC_REMOTE_PASSWORD.

Remote Directory Name for Push Mode Link Connection Report

The Remote Directory Name for Push Mode Link Connection Report installation parameter specifies an existing directory on the remote machine to which the Remote Machine Login ID for Push Mode Link Connection Report (DET.LC_REMOTE-_LOGIN) installation parameter has access.

A valid value for this parameter is a string of alphanumeric characters that represents the directory name for the remote machine.

For additional information, refer to "Link Connection Data Files" (p. 16-27).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select DET Parameters for Link Connection Report, which is option 9; then select number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.LC_REMOTE_DIRECTORY.

Data Extraction Variables for Miscellaneous Options

Enable/Disable DET Report Cron

The Enable/Disable DET Report Cron installation parameter specifies whether the Data Extraction cron should generate a report. The execution time of the cron job is 23:30 daily.

Valid values for this parameter are ON or OFF. The default is OFF, which means that a report should not be generated. Any value that is specified can be overridden when Data Extraction is executed from the command line.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select Enable/Disable DET Report Cron, which is option 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.CRON_CTRL.

Number of Retry for Push Mode

The Number of Retry for Push Mod installation parameter specifies the number of retries that should be attempted after the first **ftp** operation.

Valid values for this parameter are 0 (which indicates that a retry should NOT be attempted), 1, 2, and 3. The default is 2 retries.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select Number of Retry for Push Mode, which is option 10.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.NUM_OF_RETRY.

Retry Interval (Minutes) for Push Mode

The Retry Interval for Push Mode installation parameter specifies the number of minutes that should elapse between each retry attempt.

Valid values for this parameter are 5 minutes, through and including, 30 minutes. The default is 30 minutes.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Data Extraction Variables**, which is option 9; then select Retry Interval for Push Mode, which is option 11.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as DET.RETRY_INTERVAL.

User Services Management Variables

Password Aging Time

The Password Aging Time installation parameter specifies the number of days in the password aging period. See "Password aging" (p. 8-12).

Valid values for this parameter are 1 to 999 days. The default is 30 days.

A related platform alarm is "INVALID_PASSWD_DETECTED" (p. 42-18).

For more information regarding user passwords, refer to "Password Rules" (p. 8-11).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 1.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PASSWORD_AGING_TIME.

Password Warning Time

The Password Warning Time installation parameter specifies the number of days in which a warning message for password expiration is presented to a user. See "Password aging" (p. 8-12).

Valid values for this parameter are 1 day to 30 days. The default is 7 days, which is one week.

A related platform alarm is "INVALID_PASSWD_DETECTED" (p. 42-18).

For more information regarding user passwords, refer to "Password Rules" (p. 8-11).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 2.

When specifying option 17, **Display Current Values**, this installation parameter appears as PASSWORD_WARNING_TIME.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

Password Period of Non Use

The Password Period of Non Use installation parameter specifies the number of days in which a user is disabled for not using the management system. See "User login inactivity/non-use" (p. 8-10).

Valid values for this parameter are 1 day to 120 days. The default is 30 days.

A related platform alarm is "INVALID_PASSWD_DETECTED" (p. 42-18).

For more information regarding user passwords, refer to "Password Rules" (p. 8-11).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 3.

When specifying option 17, **Display Current Values**, this installation parameter appears as PERIOD_OF_NONUSE.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

Session Inactivity Timeout Flag

The Session Inactivity Timeout Flag installation parameter specifies whether the inactivity time-out feature should be on or off.

Valid values for this parameter are ON or OFF. The default is ON.

For more details, refer to “User login inactivity/non-use” (p. 8-10).

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 4.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) and the “Start the GUI Web Server” (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as INACTIVITY_TIMEOUT_FLAG.

Session Inactivity Timeout Period

The Session Inactivity Timeout Period installation parameter specifies the number of minutes in the time-out period.

Valid values for this parameter are 1 to 999 minutes. The default is 15 minutes.

For more details, refer to “User login inactivity/non-use” (p. 8-10).

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 5.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) and the “Start the GUI Web Server” (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as INACTIVITY_TIMEOUT.

Proprietary Agreement Warning Message Flag

The Proprietary Agreement Warning Message Flag installation parameter is used to turn the message for the proprietary agreement ON or OFF. See “Installation Parameters and the Proprietary Agreement” (p. 6-164).

Valid values for this parameter are ON or OFF. The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 6.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as WARNING_MESSAGE.

Proprietary Agreement Warning File

The Proprietary Agreement Warning File installation parameter specifies the location of the message for the proprietary agreement. See "Installation Parameters and the Proprietary Agreement" (p. 6-164).

The default location for this file is **/var/opt/lucent/ Warning_Msg** .

To create a your own proprietary agreement, see the "Create a Customized Proprietary Agreement" (p. 6-168) task.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as WARNING_FILE_LOCATION.

User Name Minimum Length

The User Name Minimum Length installation parameter specifies the minimum number of characters that can be used as a valid user name during log in to the management system.

Valid values for this parameter are 3 to 20 characters. The default is 8 characters.

A related installation parameter is "User Name Maximum Length" (p. 6-125).

For more information regarding user passwords, refer to "User ID Rules" (p. 8-9).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 8.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as USERNAME_MIN_LEN.

User Name Maximum Length

The User Name Maximum Length installation parameter specifies the maximum number of characters that can be used as a valid user name during log in to the management system.

Valid values for this parameter are 3 to 20 characters. The default is 20 characters.

A related installation parameter is "User Name Minimum Length" (p. 6-124).

For more information regarding user passwords, refer to "User ID Rules" (p. 8-9).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 9.

When specifying option 17, **Display Current Values**, this installation parameter appears as USERNAME_MAX_LEN.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

User Password Minimum Length

The User Password Minimum Length installation parameter specifies the minimum number of characters that can be used in a valid user password during log in to the management system. The stored and displayed value of the password is encrypted.

Valid values for this parameter are 8 to 15 characters. The default is 8 characters.

A related installation parameter is "User Password Maximum Length" (p. 6-126).

For more information regarding user passwords, refer to "Password Rules" (p. 8-11).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 10.

When specifying option 17, **Display Current Values**, this installation parameter appears as PASSWORD_MIN_LEN.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

User Password Maximum Length

The User Password Maximum Length installation parameter specifies the maximum number of characters that can be used in a valid user password during log in to the management system. The stored and displayed value of the password is encrypted.

Valid values for this parameter are 8 to 20 characters. The default is 20 characters.

A related installation parameter is "User Password Minimum Length" (p. 6-125).

For more information regarding user passwords, refer to "Password Rules" (p. 8-11).

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 11.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as PASSWORD_MAX_LEN.

Enable Access via CSL/SAGE

The Enable Access via CSL/SAGE installation parameter specifies whether access to the management system GUI from CSL/SAGE should be enabled.

Valid values for this parameter are YES and NO. The default is NO, which is not enabled.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 12.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as UA_SAGE.

Enable Etrust Authentication

The Enable Etrust Authentication installation parameter specifies whether the authentication interface with the Computer Associates Trust product should be enabled

Valid values for this parameter are YES and NO. The default is NO, which is not enabled.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 13.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as UA_ETRUST.

Enable Access from Metarnet

The Enable Access from Metarnet installation parameter specifies whether access to the management system GUI from Metarnet should be enabled.

Valid values for this parameter are YES and NO. The default is NO, which is not enabled.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 14.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as UA_METARNET.

Navis® EMS (SNMS) cut-through login name

The Navis® EMS (SNMS) cut-through login name installation parameter specifies a login name for Navis® EMS (SNMS) cut-through.

The initial and valid value for this parameter is “**-**”.

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 15.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) and the “Start the GUI Web Server” (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SNMSLOGIN.

Navis® EMS (SNMS) cut-through password

The Navis® EMS (SNMS) cut-through password installation parameter specifies the password that is to be used along with the Navis® EMS (SNMS) cut-through login ID. The stored and displayed value of the password is encrypted.

The initial and valid value for this parameter is “**-**”.

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **User Services Management Variables**, which is option 10, number 16.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) and the “Start the GUI Web Server” (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as SNMSPASSWD.

NBI Variables

Health Check Interval

The Health Check Interval installation parameter specifies the interval, in seconds, in which the licensed TMF814 Northbound Interface (NBI) sends a notification to the TMF814 NBI client. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are 60 to 999,999 seconds.

The default is 300 seconds, which is 5 minutes.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_HEALTH_CHECK_INTERVAL.

Ping NMS Interval

The Ping NMS Interval installation parameter specifies the interval, in seconds, in which the licensed TMF814 Northbound Interface (NBI) pings the TMF814 NBI client. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter 60 seconds to 999,999 seconds.

The default is 300 seconds, which is 5 minutes.

To modify this parameter, run the**lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 2.

The Health Check Interval installation parameter requires the system to be restarted for the parameter values to take effect.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_PING_NMS_INTERVAL.

Naming Service

The Naming Service installation parameter specifies the location of the naming service for publishing interfaces for external clients. See the "Secondary Naming Service" (p. 6-130) installation parameter to specify an additional naming service for external interfaces and see "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are LOCAL, or the prefix, host, IP address and the name of service can be specified.

The default is LOCAL, which means the local Navis® OMS naming service.

Example: If an external naming service is being used in an TMF814 NBI installation, the value for this parameter could be the following:

```
corbaloc:iiop:1.2@<IPaddress>.<PortNumber>/NameService
```

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_NAMING_SERVICE.

Secondary Naming Service

The Secondary Naming Service installation parameter specifies whether the location of a secondary naming service for external interfaces is required. See the "Naming Service" (p. 6-130) installation parameter for related parameter details and "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are NONE, or the prefix, host, IP address and the name of service can be specified. The default is NONE.

Example: If a secondary external naming service is being used in an TMF814 NBI installation, the value for this parameter could be the following:

```
corbaloc:iiop:1.2@<IPaddress>.<PortNumber>/NameService .
```

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 4.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_SECONDARY_NAMING_SERVICE.

MLSN Policy

The MLSN Policy installation parameter specifies the multi-layer subnetwork policy (MLSP) to be applied. A value of SINGLETON indicates that each NE is a subnetwork. A value of FULL_MESH indicates that all NEs are put into one subnetwork. A value of NCG_BASED indicates that the network communication groups (NCGs) are used as the subnetwork definitions. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are SINGLETON, FULL_MESH, or NCG_BASE.

Important! If MTOSI is configured in the particular installation, refer to "MTOSI-related installation parameters" (p. 19-3) for the specific setting for this installation parameter.

The default is NCG_BASED, which indicates that the NCGs are used as the subnetwork definitions.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI.MLSN_POLICY.

TMF SNC Operation

The TMF SNC Operation installation parameter supports certain TMF814 Northbound Interface and Subetwork Connection (SNC) operations. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are ENABLE_ALL or COMBINED_ONLY. When set to COMBINED_ONLY, createAndActivateSNC and deactivateAndDeleteSNC are supported; but, createSNC, activateSNC, deactivateSNC and deleteSNC are not supported. When set to ENABLE_ALL, then all operations (createAndActivateSNC, deactivateAndDeleteSNC, createSNC, activateSNC, deactivateSNC, and deleteSNC) are supported.

The default is COMBINED_ONLY.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_TMF_SNC_OPS.

TMF Unmanaged Domain Support

The TMF Unmanaged Domain Support installation parameter enables or disables the unmanaged domain support over the TMF814 Northbound Interface. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are ENABLED and DISABLED.

The default is ENABLED.

Important! If MTOSI is configured in the particular installation, refer to "MTOSI-related installation parameters" (p. 19-3) for the specific setting for this installation parameter.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_BBOX_SUPPORT.

TMF SNC End Point Rules

The TMF SNC End Point Rules installation parameter defines the SNC end point rules for the TMF814 Northbound Interface. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are DEFAULT and BBOX_NOT_ALLOWED.

The default is DEFAULT.

Important! If MTOSI is configured in the particular installation, refer to "MTOSI-related installation parameters" (p. 19-3) for the specific setting for this installation parameter.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_SNC_ENDPOINT_RULES.

TMF SNC Naming

The TMF SNC Naming installation parameter defines the SNC naming policy for the TMF northbound interface. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are STANDARD and NON-STANDARD.

The default is STANDARD.

Important! If MTOSI is configured in the particular installation, refer to "MTOSI-related installation parameters" (p. 19-3) for the specific setting for this installation parameter.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 9.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_SNC_NAMING.

TMF G7 - Contained VCG Servers

The TMF G7 - Contained VCG Servers installation parameter determines whether Virtual Contatenation Group (VCG) servers in CMISE NEs are to be CTPs or FTPs and CTPs.

Valid values for this parameter are YES, which means that the VCG servers in CMISE NEs are to be CTPs contained in the VCG FTP, or NO, which means that the VCG servers in the CMISE NEs are to be FTPs and CTPs in a MUX group relationship with the VCG FTP. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 10.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_CONTAINED_VCG_SERVERS.

TMF G7 - Reissue Alarms when Correlation Changes

The TMF G7 - Reissue Alarms when Correlation Changes installation parameter enables or disables the resending of alarms over the northbound G7 interface if their correlation state changes. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are YES to enable the resending of alarms or NO to disable the resending of alarms. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 11.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as G7.REISSUE_ALARMS.

TMF G7 - Enable TMF G7 Interface

The TMF G7 - Enable TMF G7 Interface installation parameter enables or disables the northbound TMF G7 interface. See "TMF814 Northbound Interface Concepts" (p. 18-2) for more information about the TMF814 NBI.

Valid values for this parameter are YES to enable the interface or NO to disable the interface. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **NBI Variables**, which is option 11, number 12.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as G7.ENABLE.

TMF - Raise Alarms During Connection Provisioning

TMF - Raise Alarms During Connection Provisioning installation parameter specifies whether alarms should be enabled or disabled while provisioning connections.

Valid values for this parameter are ENABLED and DISABLED. The default is ENABLED.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 13.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI_PROV_ALARMS.

Use G7 CTP Naming Format on TMF814 Interface

The Use G7 CTP Naming Format on TMF814 Interface installation parameter specifies whether G7 naming semantics for CTPs on the TMF814 Northbound Interface should be enabled or disabled.

Valid values for this parameter are YES and NO. The default is NO, which disables the G7 naming semantics.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 14.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI.G7_CTP_NAMING.

ASIM - Enable Alarm Server interface

The ASIM - Enable Alarm Server interface installation parameter enables the northbound Alarm Server Interface. The ASIM - Enable Alarm Server interface installation parameter is applicable for 1350OMS only.

Valid values for this parameter are YES and NO. The default is NO, which disables the northbound Alarm Server Interface.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 15.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ASIM.ENABLE.

ASIM - EMS identifier

The ASIM - EMS identifier installation parameter sets the EMS Identifier in the Alarm Server interface. The ASIM - EMS identifier installation parameter is applicable for 1350OMS only.

Valid values for this parameter are 1 through 10000, which allows the user to set an exact Identifier (1 through 10000). The default is 1.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 16.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ASIM.EMSID.

Drop connections ending at CTP of SHDSL PTP

The Drop connections ending at CTP of SHDSL PTP installation parameter determines whether to drop connections ending at CTP of SHDSL PTP.

Valid values for this parameter are YES and NO. The default is YES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 17.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NBI.DROP_SHDSL_CTP.

ASIM - Forward physical alarms to AS

The ASIM - Forward physical alarms to AS installation parameter enables physical alarms to be forwarded to AS when set to YES.

Valid values for this parameter are YES and NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select the **NBI Variables** option, which is option 11, number 18.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the GUI Web Server" (p. 9-9) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ASIM.PHYLINK_ALM.

TIM Variables

TIM Username

The TIM Username installation parameter specifies the username for the TIM interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

The default is tim.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.USERNAME.

TIM Password

The TIM Password installation parameter specifies the password for the TMN Integration Module (TIM) interface. The stored and displayed value of the password is encrypted. See “TIM Interface for a Northbound OSS” (p. 17-3) for more information about the TIM interface.

The default is tim123.

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **TIM Variables**, which is option 12, number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PASSWORD.

TIM Timezone

The TIM Timezone installation parameter specifies the time zone (time stamp) to be used for alarms sent on the TMN Integration Module (TIM) interface. See “TIM Interface for a Northbound OSS” (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are UTC (Coordinated Universal Time) and LOCAL. The default is LOCAL.

Note : All time stamps are in the format of the following:

MM-DD-YYYY HH:MM:SS

To modify this parameter, run the **lt_param_reconfig** tool; see the “Modify an Installation Parameter” (p. 6-167) task. Select **TIM Variables**, which is option 12, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to “Restarting of and interaction with system components” (p. 6-11) and the “Start the Platform” (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.TIMEZONE.

TIM FM Filtering

The TIM FM Filtering installation parameter defines whether the service affecting (SA) or the service affecting and non-service affecting (N-SA) alarm set is to be reported on the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are SA, which is service affecting, and SA_AND_NSA, which is service affecting and non-service affecting (N-SA). The default is SA_AND_NSA.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 4.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.FM_FILTERING.

TIM Heartbeat Interval

The TIM Heartbeat Interval installation parameter specifies the time in minutes between TMN Integration Module (TIM) interface heartbeats, which are used to signal the health of the interface.

Note: The format of the heartbeat message adheres to the following: <*timestamp*> <*text*>. For example:

```
01-01-2004 01:01:01
```

```
The Link is UP
```

See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are 1 to 60 minutes. The default is 10 minutes.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.HEARTBEAT_INTERVAL.

TIM Alarm Severity Terminology

The TIM Alarm Severity Terminology installation parameter specifies the Alarm Severity Terminology for the TMN Integration Module (TIM) interface. If the alarm terminology is set to PDI, alarm classifications are prompt (P), deferred (D), or informational (I). If the alarm terminology is set to CMMW, the alarm classifications are critical (C), major (J), minor (N), warning (W), or indeterminate (U). See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are PDI or CMMW. The default is PDI.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.ALM_SEV_TERMINOLOGY.

TIM Synchronous Data Transmission Terminology

The TIM Synchronous Data Transmission Terminology installation parameter specifies the Data Transmission Terminology for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are SDH or SONET. The default is SDH.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.TERMINOLOGY_PREF.

TIM Enable PSEs from Equipment Switch as Alarms

The TIM Enable PSEs from Equipment Switch as Alarms installation parameter processes PSEs from equipment switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_EQM.

TIM Enable PSEs from MSSPRING Switch as Alarms

The TIM Enable PSEs from MSSPRING Switch as Alarms installation parameter processes PSEs from MSSPRING switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 9.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_MSSPRING.

TIM Enable PSEs from RPR Switch as Alarms

The TIM Enable PSEs from RPR Switch as Alarms installation parameter processes PSEs from RPR switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 10.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_RPR.

TIM Enable PSEs from TDM HO SNCP Switch as Alarms

The TIM Enable PSEs from TDM HO SNCP Switch as Alarms installation parameter processes PSEs from TDM HO SNCP switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 11.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_TDM_HO_SNCP.

TIM Enable PSEs from TDM MSP Switch as Alarms

The TIM Enable PSEs from TDM MSP Switch as Alarms installation parameter processes PSEs from TDM MSP switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 12.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_TDM_MSP.

TIM Enable PSEs from WDM HO SNCP Switch as Alarms

The TIM Enable PSEs from WDM HO SNCP Switch as Alarms installation parameter processes PSEs from WDM HO SNCP switches as alarms for the TMN Integration Module (TIM) interface. See "TIM Interface for a Northbound OSS" (p. 17-3) for more information about the TIM interface.

Valid values for this parameter are YES or NO. The default is NO.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **TIM Variables**, which is option 12, number 13.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as TIM.PSE_PROCESS_WDM_HO_SNCP.

Northbound SNMP Variables

SNMP Version

The SNMP Version installation parameter specifies the Simple Network Management Protocol (SNMP) version to be supported for the northbound interface. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

Important! The setting of this installation parameter directly affects the validity and setting of the "SNMP Security Level" (p. 6-146) installation parameter.

Valid values for this parameter are V2C and V3. The default is V3.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_VERSION.

SNMP Address/Port Number

The SNMP ADDRESS/PORT NUMBER installation parameter identifies the IP address for the system that is to receive Simple Network Management Protocol (SNMP) traps from the management system for the northbound interface. For additional information about the feature, refer to "SNMP Interface" (p. 17-5).

The format for the installation parameter is the following:

IP_address/port_number

For example:

12.34.56.78/9000

A value of 0.0.0.0/-1 disables the sending of traps.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 2.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_ADDR_1.

SNMP Security Name

The SNMP Security Name installation parameter identifies the community name, which is effectively the password, for the northbound Simple Network Management Protocol (SNMP) interface. For additional information about the feature, refer to "SNMP Interface" (p. 17-5).

The valid value for this parameter is the name/password for the northbound SNMP interface, or the word, *NONE*, which means that the name/password has not been specified and the interface will not accept requests. The default is NONE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_COMM_NAME.

SNMP Security Level

The SNMP Security Level installation parameter specifies the Simple Network Management Protocol (SNMP) security level for the northbound SNMP interface. This installation parameter is not applicable if the "SNMP Version" (p. 6-145) installation parameter is set to version 2C, which is no authentication and no privacy. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

Important! The setting of this installation parameter directly affects the settings or the defaults of the following installation parameters:

- "SNMP Authentication Protocol" (p. 6-147)
- "SNMP Authentication Password" (p. 6-148)

- "SNMP Privacy Protocol" (p. 6-148)
- "SNMP Privacy Password" (p. 6-149)

Valid values for this parameter are NOAUTH_NOPRIV (no authentication and no privacy), AUTH_NOPRIV (authentication and no privacy), and AUTH_PRIV (authentication and privacy). The default is AUTH_PRIV, which is authentication and privacy.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 4.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_SECURITY_LEVEL.

SNMP Authentication Protocol

The SNMP Authentication Protocol installation parameter specifies the Simple Network Management Protocol (SNMP) authentication protocol that is to be used if the security level is set to enable authentication for the northbound interface. For more details about the security level, refer to the "SNMP Security Level" (p. 6-146) installation parameter. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

Valid values for this parameter are MD5 and SHA. The default is MD5, which means the MD5 authentication protocol is to be used.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_AUTH.

SNMP Authentication Password

The SNMP Authentication Password installation parameter specifies the Simple Network Management Protocol (SNMP) authentication password that is to be used if the security level is set to enable authentication for the northbound interface. The stored and displayed value of the password is encrypted. For more details about the security level, refer to the "SNMP Security Level" (p. 6-146) installation parameter. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

A valid value for this parameter is a password of at least 8 characters up to a maximum of 60 characters. For additional security, screen output is suppressed while this password is being modified. The password is initially set to NONE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_AUTH_PASSWD.

SNMP Privacy Protocol

The SNMP Privacy Protocol installation parameter specifies the Simple Network Management Protocol (SNMP) privacy protocol to be used if the security level is set to enable privacy for the northbound interface. For more details about the security level, refer to the "SNMP Security Level" (p. 6-146) installation parameter. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

Valid values for this parameter are DES, AES128, AES192, and AES256. The default is DES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Northbound SNMP Variables**, which is option 13, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_PRIV.

SNMP Privacy Password

The SNMP Privacy Password installation parameter specifies the Simple Network Management Protocol (SNMP) privacy password to be used if the security level is set to enable privacy for the northbound interface. The stored and displayed value of the password is encrypted. For more details about the security level, refer to the "SNMP Security Level" (p. 6-146) installation parameter. For more details about SNMP, refer to "SNMP Interface" (p. 17-5).

A valid value for this parameter is a password of at least 8 characters up to a maximum of 60 characters. For additional security, screen output is suppressed while this password is being modified. The password is initially set to NONE.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select Select **Northbound SNMP Variables**, which is option 13, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as NB_SNMP_PRIV_PASSWD.

Southbound SNMP Variables

SNMP Security Name

The SNMP Security Name installation parameter specifies the community name for the Simple Network Management Protocol (SNMP) interface for the southbound interface.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

The initial value for this parameter is set to **snmpsna**.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 1.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_USER_NAME.

SNMP Security Level

The SNMP Security Level installation parameter specifies the Simple Network Management Protocol (SNMP) security level for the southbound SNMP interface.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

Valid values for this parameter are NOAUTH_NOPRIV (no authentication and no privacy), AUTH_NOPRIV (authentication and no privacy), and AUTH_PRIV (authentication and privacy). The default is NOAUTH_NOPRIV, which is no authentication and no privacy.

Important! The setting of this installation parameter directly affects the settings or the defaults of the following installation parameters:

- "SNMP Authentication Protocol" (p. 6-150)
- "SNMP Authentication Password" (p. 6-151)
- "SNMP Privacy Protocol" (p. 6-151)
- "SNMP Privacy Password" (p. 6-152)

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 2.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_SECURITY_LEVEL.

SNMP Authentication Protocol

The SNMP Authentication Protocol installation parameter specifies the Simple Network Management Protocol (SNMP) authentication protocol that is to be used if the security level is set to enable authentication for the southbound interface. For more details about the security level, refer to the "SNMP Security Level" (p. 6-150) installation parameter.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

Valid values for this parameter are MD5 and SHA. The default is MD5, which means the MD5 authentication protocol is to be used.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_AUTH.

SNMP Authentication Password

The SNMP Authentication Password installation parameter specifies the Simple Network Management Protocol (SNMP) authentication password that is to be used if the security level is set to enable authentication for the southbound interface. The stored and displayed value of the password is encrypted. For more details about the security level, refer to the "SNMP Security Level" (p. 6-150) installation parameter.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

A valid value for this parameter is a password of at least 8 characters. The password is initially set to the following encrypted values:

Authentication password: **sna!1234**

Note: For additional security, screen output is suppressed while this password is being modified. Users must configure the NE to match this encrypted value so they must either know the password or choose a password of their own.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_AUTH_PASSWD.

SNMP Privacy Protocol

The SNMP Privacy Protocol installation parameter specifies the Simple Network Management Protocol (SNMP) privacy protocol to be used if the security level is set to enable privacy for the southbound interface. For more details about the security level, refer to the "SNMP Security Level" (p. 6-150) installation parameter.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

The valid value for this parameter is DES. The default is DES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 5.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_PRIV.

SNMP Privacy Password

The SNMP Privacy Password installation parameter specifies the Simple Network Management Protocol (SNMP) privacy password to be used if the security level is set to enable privacy for the southbound interface. The stored and displayed value of the password is encrypted. For more details about the security level, refer to the "SNMP Security Level" (p. 6-150) installation parameter.

Note: This installation parameter is only configured when OMS is an management system for transport for OMC-RAN.

A valid value for this parameter is a password of at least 8 characters. The password is initially set to the following encrypted values:

Privacy password: **ethernet15000**

Note: For additional security, screen output is suppressed while this password is being modified. Users must configure the NE to match this encrypted value so they must either know the password or choose a password of their own.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Southbound SNMP Variables**, which is option 14, number 6.

This parameter does not require any system restart (**None**) for the parameter values to take effect.

When specifying option 17, **Display Current Values**, this installation parameter appears as SB_SNMP_PRIV_PASSWD.

External Authentication Variables

Authentication Method

The Authentication Method installation parameter specifies the mode of user authentication.

Valid values for this parameter are either STD (which is the standard internal scheme) or RADIUS or RSA (which are two types of external authentication servers). The default is STD.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_METHOD.

Allow Local GUI User Authentication

The Allow Local GUI User Authentication installation parameter specifies whether a remote authentication server should enable the local authentication of GUI users when the "Authentication Method" (p. 6-153) (AUTH_METHOD) installation parameter is not of the standard internal scheme (STD). Only user accounts that are marked as local accounts are locally authenticated.

Valid values for this parameter are YES or NO. The default is YES.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 2.

This parameter requires the GUI web server (GWS) to be restarted for the parameter values to take effect. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_GUI_USERS_LOCALLY.

Default User Role

The Default User Role installation parameter specifies the default user role for accounts that are generated automatically as a result of an external authentication server.

The value for this parameter must exactly match one of the user role names defined in OMS. The default is NOC Operator. Refer to "User Role Profile Concepts" (p. 7-2) for details.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 3.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as USER_ROLE_DEFAULT.

Default User Domain

The Default User Domain installation parameter specifies whether an automatically generated account should be restricted by the domain partitions or should be allowed global access.

The valid values are **RESTRICTED** or **GLOBAL**. The default is **GLOBAL**.

The domains to which a restricted user has access are defined using the domain partitioning feature.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 4.

This parameter does not require any system restart (**None**) for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as USER_DOMAIN_DEFAULT.

Authentication Server Retries

The Authentication Server Retries installation parameter specifies the number of retries that are used when calling the authentication server.

Valid values for this parameter are 1 through 10, which allows the user to set an exact number of retries (1 through 10). The default is 3.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_RETRIES.

Authentication Server Timeout in Seconds

The Authentication Server Timeout in Seconds installation parameter specifies the timeout in seconds for authentication server calls.

Valid values for this parameter are 1 through 60 seconds. The default is 30 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_TIMEOUT.

Authentication Server Selection Policy

The Authentication Server Selection Policy installation parameter specifies the policy for the selection of authentication servers.

Valid values for this parameter are SEQ (sequential where the next server is called when the first server fails) or RR (round robin where each call goes to the next server). The default is SEQ.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_SELECT.

Address of External Server 1

The Address of External Server 1 installation parameter specifies the IP address and port number for an authentication server if it is present.

Valid values for this parameter are the IP address and port number for an authentication server, specified in the format of:

nn.nn.nn.nn:p

where: p is the port number.

The default is -- (a double-hyphen), which indicates that an authentication server is not present.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 8.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_ADDRESS_1.

Shared Secret for Server 1

The Shared Secret for Server 1 installation parameter specifies the shared secret, which is an encrypted value, for this authentication server.

The valid value for this parameter is an encrypted string. The default is -- (double-hyphen), which indicates that a shared secret for this authentication server is not specified. The shared secret has a maximum length of 70 characters.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 9.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_SS_1.

Address of External Server 2

The Address of External Server 2 installation parameter specifies the IP address and port number for an authentication server if it is present.

Valid values for this parameter are the IP address and port number for an authentication server, specified in the format of:

nn.nn.nn.nn:p

where: p is the port number.

The default is -- (a double-hyphen), which indicates that an authentication server is not present.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 10.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_ADDRESS_2.

Shared Secret for Server 2

The Shared Secret for Server 2 installation parameter specifies the shared secret, which is an encrypted value, for this authentication server.

The valid value for this parameter is an encrypted string. The default is -- (double-hyphen), which indicates that a shared secret for this authentication server is not specified. The shared secret has a maximum length of 70 characters.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 11.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_SS_2.

Address of External Server 3

The Address of External Server 3 installation parameter specifies the IP address and port number for an authentication server if it is present.

Valid values for this parameter are the IP address and port number for an authentication server, specified in the format of:

nn.nn.nn.nn:p

where: p is the port number.

The default is -- (a double-hyphen), which indicates that an authentication server is not present.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 12.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_ADDRESS_3.

Shared Secret for Server 3

The Shared Secret for Server 3 installation parameter specifies the shared secret, which is an encrypted value, for this authentication server.

The valid value for this parameter is an encrypted string. The default is -- (double-hyphen), which indicates that a shared secret for this authentication server is not specified. The shared secret has a maximum length of 70 characters.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 13.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_SS_3.

Address of External Server 4

The Address of External Server 4 installation parameter specifies the IP address and port number for an authentication server if it is present.

Valid values for this parameter are the IP address and port number for an authentication server, specified in the format of:

nn.nn.nn.nn:p

where: p is the port number.

The default is -- (a double-hyphen), which indicates that an authentication server is not present.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 14.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_ADDRESS_4.

Shared Secret for Server 4

The Shared Secret for Server 4 installation parameter specifies the shared secret, which is an encrypted value, for this authentication server.

The valid value for this parameter is an encrypted string. The default is -- (double-hyphen), which indicates that a shared secret for this authentication server is not specified. The shared secret has a maximum length of 70 characters.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 15.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as AUTH_SERVER_SS_4.

Vendor Private Enterprise Number

The Vendor Private Enterprise Number installation parameter specifies the Private Enterprise Number for Alcatel-Lucent as assigned by the IANA. The private enterprise number is used on the RADIUS interface.

The valid value for this parameter is a number from 0 to 16777216. The default is 1751.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **External Authentication Variables**, which is option 15, number 16.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as OMS_VENDOR_ID.

Preplan Restoration Variables

Alarm Triggered Preplan Restoration

The Alarm Triggered Preplan Restoration installation parameter is used to enable or disable the alarm triggering of pre-plan restoration. Contrast with "Automatic Routing of Preplan Restoration Connections" (p. 6-161). Refer to "OMS_PREPLAN license" (p. 5-13) for additional details regarding the Preplan Restoration feature. In addition, refer to the "Preplan Management user task" (p. 7-20) and "Preplan Management (View Only) user task" (p. 7-20) for additional details regarding the restrictions that each user task imposes.

Valid values for this parameter are ON and OFF.

The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 1.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ALARM_TRIGGERED_PREPLAN.

Automatic Routing of Preplan Restoration Connections

The Automatic Routing of Preplan Restoration Connections installation parameter is used to enable or disable the automatic routing algorithm for Preplan Restoration. Contrast with "Alarm Triggered Preplan Restoration" (p. 6-160). Refer to the "Preplan Management user task" (p. 7-20) and "Preplan Management (View Only) user task" (p. 7-20) for additional details regarding the restrictions that each user task imposes.

Valid values for this parameter are ON and OFF.

The default is OFF.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 2.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as ALGORITHM_TRIGGERED_PREPLAN.

Preplan log retention period in days

The Preplan Log Retention Period installation parameter specifies the number of days for which preplan records are to be retained.

Valid values for this parameter are 1 to 90 days. The default is 35 days.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 3.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits. Refer to "Restarting of and interaction with system components" (p. 6-11) and the "Start the Platform" (p. 9-5) task for details.

When specifying option 17, **Display Current Values**, this installation parameter appears as KEEP_PREPLAN_LOG_ENTRIES.

Number of Retained History Orders

The Number of Retained History Orders installation parameter specifies the number of history orders that are to be retained.

Valid values for this parameter are 1 to 100.

The default is 0 history orders.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 4.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits.

When specifying option 17, **Display Current Values**, this installation parameter appears as PREPLAN_HISTORY_ORDERS.

Hold Off Time for Alarm Triggered Restoration

The Hold Off Time for Alarm Triggered Restoration installation parameter specifies the number of seconds that constitute the hold-off time for alarm triggered preplan restoration.

Valid values for this parameter are 1 to 180 seconds.

The default is 30 seconds.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 5.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits.

When specifying option 17, **Display Current Values**, this installation parameter appears as PREPLAN_HOLDOFF.

Maximum number of member pairs per plan

The Maximum number of member pairs per plan installation parameter specifies the maximum number of member pairs in a preplan plan.

Valid values for this parameter are 1 to 70 member pairs.

The default is 70 member pairs.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 6.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits.

When specifying option 17, **Display Current Values**, this installation parameter appears as PREPLAN_MAX_PLAN.

Maximum number of plans per preplan group

The Maximum number of plans per preplan group installation parameter specifies the maximum number of member of a preplan plans in a preplan group.

Valid values for this parameter are 1 to 15 plans.

The default is 15 plans.

To modify this parameter, run the **lt_param_reconfig** tool; see the "Modify an Installation Parameter" (p. 6-167) task. Select **Preplan Restoration Variables**, which is option 16, number 7.

This parameter requires the OMS platform (which includes the GWS) to be restarted for the parameter values to take effect. In addition, none of NA types use this installation parameter; therefore, an automatic download of parameters to the NAs does not occur when lt_param_reconfig exits.

When specifying option 17, **Display Current Values**, this installation parameter appears as PREPLAN_MAX_GROUP.

Installation Parameters and the Proprietary Agreement

Definition of a proprietary agreement

A proprietary agreement is block of legal text that can be displayed each time a user logs into the management system. The user can accept or decline the proprietary agreement. If the user accepts the agreement (positive response), then the user is granted access to the management system. If the user declines the agreement (negative response), then the user is logged off the system.

Installation parameters for the proprietary agreement

A pair of installation parameters controls the proprietary agreement:

- The installation parameter "Proprietary Agreement Warning Message Flag" (p. 6-123) turns the propriety agreement feature on or off for all users.
- The installation parameter "Proprietary Agreement Warning File" (p. 6-124) specifies the path and file name for the content of the proprietary agreement.

Proprietary agreement file

The management system enables the system administrator to change the text of the proprietary agreement by creating an ASCII file that contains the new content of the agreement.

The ASCII file can be created using any text editor, or the file can be created on the HP® server using one of the UNIX® editors, such as **vi**.

For readability and appearance, the file should not exceed 1024 characters; however, a strict file size limit is not imposed—the scroll bar merely appears and allows the user to display the entire message. The text of the file should conclude with the question:

```
Do you agree?
```

View the Parameter Settings of an Installation Parameter

When to use

Use this task to view the parameter settings of an installation parameter.

Related information

See the following topic in this document:

- "lt_param_reconfig and its menu options" (p. 6-2)

Before you begin

This task can be completed in one of two methods.

Task: Method 1

Complete the following steps to view the parameter settings of an installation parameter.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Ensure that the management system application is running.

3 At the prompt, enter the following command line:

```
/opt/lucent/platform/bin/lt_param_reconfig -L
```

Result: The current setting of all parameter values is displayed.

END OF STEPS

Task: Method 2

Complete the following steps to view the parameter settings of an installation parameter.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Ensure that the management system application is running.

3 At the prompt, enter the following command line:

```
/opt/lucent/platform/bin/lt_param_reconfig
```

Result: A menu of all tunable parameters is displayed.

4 Enter option 15 to display current values: `16`

Result: The current settings for all parameter values are displayed.

END OF STEPS

Modify an Installation Parameter

When to use

Use this task to modify an installation parameter.

Related information

See the following topic in this document:

- "lt_param_reconfig and its menu options" (p. 6-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view or modify an installation parameter.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Ensure that the management system application is running.

3 At the prompt, enter the following command line:

```
/opt/lucent/platform/bin/lt_param_reconfig
```

Result: A menu of all tunable parameters is displayed.

4 Follow the menu prompts to change the particular installation parameter or parameters.

Result: The parameter is changed. Depending on the type of installation parameter that was changed, many times the redefined parameter does not take effect until the management system is restarted; see the "Start the Platform" (p. 9-5) task.

END OF STEPS

Create a Customized Proprietary Agreement

When to Use

Use this task to create a file that contains customized content for the proprietary agreement.

Related information

See the following topics in this document:

- "Installation Parameters and the Proprietary Agreement" (p. 6-164)
- "Proprietary Agreement Warning Message Flag" (p. 6-123)
- "Proprietary Agreement Warning File" (p. 6-124)
- "Modify an Installation Parameter" (p. 6-167)
- "Start the Platform" (p. 9-5)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to create the proprietary agreement.

1 From the machine on which the management system is running, log in as **`root`**.

2 The name and the location of the file that contains the proprietary agreement message is specified in the "Proprietary Agreement Warning File" (p. 6-124) installation parameter. The default location of this file can be found using the following path:

var/opt/lucent/Warning_Msg

Change directories to that directory.

3 Using the **vi** editor, create a file with the name that contains the proprietary agreement that is to appear during the user login sequence.

The file should not exceed 1024 characters for the sake of readability and appearance. Also, it needs a **/n** for a line return. In addition, the text of the file should conclude with the question: `Do you agree?`

4 Save the file and exit the editor.

Result: The proprietary agreement is created.

5 The installation parameter "Proprietary Agreement Warning Message Flag" (p. 6-123) turns the propriety agreement feature on or off for all users. For the changed proprietary agreement to take effect, this parameter must be turned on.

Use the "Modify an Installation Parameter" (p. 6-167) task to turn "Proprietary Agreement Warning Message Flag" (p. 6-123) on.

6 Use the "Start the Platform" (p. 9-5) task to restart the application.

Result: The application is started/restarted, which takes up to 15 minutes to complete.

END OF STEPS

7 User Role Profiles

Overview

Purpose

This chapter contains the conceptual information and tasks associated with user role profiles.

Contents

User Role Profile Concepts

User role profile functions

A user role profile is the set of tasks that a particular user login can perform. The set of tasks available for any user role profile is determined by the product licenses that are currently installed for the management system. (Refer to "Available Licenses" (p. 5-4) and "Licenses and user role profiles" (p. 5-2).) These tasks govern user access to the management system, which specifically includes which pages and icons are displayed and which actions can be performed; thus, user role profiles are an inherent security mechanism for the management system.

Creation of a user role profile is based on the tasks that a user is allowed to perform. For example, the user role profile for a network supervisor could have both system administration and provisioning types of tasks included so the supervisor could perform these functions within the domain of one user ID.

User role profile functions are supported from the following pages of the management system:

Administration > Users > User Role Profiles

User accounts in the LDAP database

User management is handled by the Lightweight Directory Access Protocol (LDAP) software. Each created user account is stored in the LDAP database.

Two types of user role profiles

The management system offers two types of user role profiles:

- *Factory-defined user role profiles*, which are predefined profiles that come installed with each management system
- *User-defined user role profiles*, which are customized profiles that the system administrator (the NOC Administrator) creates for one or more management system users

Factory-Defined User Role Profiles

Types of factory-defined user role profiles

The management system is installed with these factory-defined user role profiles:

- Network Operations Center Administrator (NOC Administrator)
- Network Operations Center Expert Operator (NOC Expert Operator)
- Network Operations Center Operator (NOC Operator)

These factory-defined user role profiles cannot be modified or deleted from the management system. The NOC Administrator can copy any factory-defined user role profile and modify it to create a user-defined user role profile. See the "Copy a User Role Profile" (p. 7-24) task.

NOC Administrator profile

Depending on the product licenses that are currently installed for the management system, the default tasks that are assigned to the factory-defined user role profile for the NOC Administrator are the following:

- "All User Activity Log user task" (p. 7-8)
- "Database Back Up Administration user task" (p. 7-10)
- "Fault Management Logs Administration user task" (p. 7-14)
- "Login Session Administration user task" (p. 7-14)
- "Own Administration user task" (p. 7-18)
- "Security Log user task" (p. 7-21)
- "System Administration user task" (p. 7-21)
- "System Alarm Supervision user task" (p. 7-22)
- "TMF Session Administration user task" (p. 7-22)
- "User Administration user task" (p. 7-22)

NOC Expert Operator profile

Depending on the product licenses that are currently installed for the management system, the default tasks that are assigned to the factory-defined user role profile for the NOC Expert Operator are the following:

- "Alarm Supervision user task" (p. 7-7)
- "All TL1 Macro Files Management user task" (p. 7-7)
- "Area and Aggregate Management user task" (p. 7-8)
- "Connection Management user task" (p. 7-9)
- "Domain Administration user task" (p. 7-10)
- "Ethernet Administration user task" (p. 7-11)

- "Ethernet Element Management user task" (p. 7-11)
- "Ethernet Hub-and-Spoke Service Provisioning user task" (p. 7-12)
- "Ethernet Infrastructure Provisioning user task" (p. 7-12)
- "Ethernet Non-Switched Service Provisioning user task" (p. 7-13)
- "Ethernet Switched Service Provisioning user task" (p. 7-13)
- "Global UI Settings user task" (p. 7-14)
- "Login Session Administration user task" (p. 7-14)
- "My Preferences user task" (p. 7-15)
- "NE Engineering user task" (p. 7-15)
- "NE Management Access user task" (p. 7-16)
- "NE Management user task" (p. 7-17)
- "NE Software Management user task" (p. 7-17)
- "OMS ASAP Management user task" (p. 7-18)
- "Own Administration user task" (p. 7-18)
- "Own User Activity Log user task" (p. 7-19)
- "Performance Monitoring user task" (p. 7-19)
- "Preplan Management user task" (p. 7-20)
- "Profile Management user task" (p. 7-20)

NOC Operator profile

Depending on the product licenses that are currently installed for the management system, the default tasks that are assigned to the factory-defined user role profile for the NOC Operator are the following:

- "Alarm Supervision user task" (p. 7-7)
- "Area and Aggregate Management (View Only) user task" (p. 7-8)
- "Connection Management user task" (p. 7-9)
- "Ethernet Element Management user task" (p. 7-11)
- "Ethernet Hub-and-Spoke Service Provisioning user task" (p. 7-12)
- "Ethernet Infrastructure Provisioning user task" (p. 7-12)
- "Ethernet Non-Switched Service Provisioning user task" (p. 7-13)
- "Ethernet Switched Service Provisioning user task" (p. 7-13)
- "Login Session Administration user task" (p. 7-14)
- "My Preferences user task" (p. 7-15)
- "NE Engineering user task" (p. 7-15)
- "NE Management user task" (p. 7-17)
- "NE Software Management user task" (p. 7-17)

- "Own Administration user task" (p. 7-18)
- "Own TL1 Macro Files Management user task" (p. 7-18)
- "Own User Activity Log user task" (p. 7-19)
- "Performance Monitoring (View-Only) user task" (p. 7-19)
- "Preplan Management user task" (p. 7-20)
- "Profile Management (View Only) user task" (p. 7-21)

User-Defined User Role Profiles

Creation of user-defined user role profiles

The NOC Administrator creates a user-defined user role profile from the set of tasks available on the User Role Profile page. This set of tasks is governed by the product licenses that are currently installed for the management system. (Refer to "Available Licenses" (p. 5-4) and "Licenses and user role profiles" (p. 5-2).)

The list of available user role profile tasks includes all tasks that are available for the NOC Administrator, NOC Expert Operator, NOC Operator, along with the numerous unassigned tasks; therefore, a user-defined user role profile can include any combination of the following:

- any and/or all tasks that are assigned to any and/or all factory-defined user role profiles
- any and/or all tasks that are considered to be unassigned; see "Unassigned user tasks" (p. 7-5)
- any subset of tasks that is a assigned to any factory-defined user role profile or profiles

Number of user tasks that can be assigned

The number of tasks that can be assigned to a user is only limited by the user function and the security level that is to be imposed on the management system. The number of tasks that can be assigned to a user is not limited to any management system rule or convention; meaning, if needed, one user could have a user-defined user role profile that contains all of the tasks that are assigned to a NOC Administrator, a NOC Expert Operator, and a NOC Operator.

Unassigned user tasks

Unassigned user tasks are those user tasks that have not been assigned to a factory-defined user role profile. In many instances, unassigned tasks are view-only tasks; meaning, they have read-only privileges.

Depending on the product licenses that are currently installed for the management system, the following tasks have not be assigned to a factory-defined user role profile:

- “Alarm Observation user task” (p. 7-7)
- “Connection Management (View-Only) user task” (p. 7-9)
- “Database Back Up Administration (View-Only) user task” (p. 7-10)
- “Ethernet Element Management (View-Only) user task” (p. 7-12)
- “Ethernet (View-Only) user task” (p. 7-13)
- “NE Engineering (View-Only) user task” (p. 7-16)
- “NE Management (View-Only) user task” (p. 7-17)
- “NE Software Management (View-Only) user task” (p. 7-18)
- “Preplan Management (View Only) user task” (p. 7-20)
- “SHDSL Device Password Modification user task” (p. 7-21)

Note: Any user task that has read/write privileges has precedence over the corresponding unassigned task that has read-only privileges.

User-defined user role profile nomenclature

A user-defined user role profile must be named with a unique string of 1 to 50 alphanumeric characters, excluding the following special characters:

*** < > ? “ ” ‘ % **

If one of these special characters is used, the management system displays an error message in the message zone to inform the user that these characters cannot be used when naming a user-defined user role profile.

User-defined user role profile manipulation

Unlike the factory profiles that cannot be deleted, user-defined user role profiles can be deleted from the management system database. In addition, a user-defined user role profile can be copied and then modified if needed.

User Tasks

Alarm Observation user task

The Alarm Observation user task permits enterprise network management (ENM) users to view Alarm Summaries, Alarm Logs, the Alarm List, and Protection Switch Events (PSEs).

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Alarm Observation user task is an unassigned, read-only task that is available to any user-defined user role profile that has a need for this task.

Alarm Supervision user task

The Alarm Supervision user task permits enterprise network management (ENM) users to undertake alarm surveillance activities that require the full functionality of alarm management, including Protection Switch Events (PSEs).

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Alarm Supervision user task, which is a read-write task, is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The All Supervision user task is available with the "OMS_CORE license" (p. 5-5).

All TL1 Macro Files Management user task

The All TL1 Macro Files Management user task enables users to view, modify, and delete all TL1 Macro Files.

The All TL1 Macro Files Management user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The All TL1 Macro Files Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

All User Activity Log user task

The All User Activity Log user task enables users to view the User Activity Log of all users.

The All User Activity Log user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The All User Activity Log user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Area and Aggregate Management user task

The Area and Aggregate Management user task permits users to view, create, delete, and modify an area or an aggregate.

The Area and Aggregate Management user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The Area and Aggregate Management user task is not available to Domain users; that is, those users who have the Domain attribute of their user accounts set to *Restricted*.

The Area and Aggregate Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

For more information about Domain Partitioning Management, refer to "OMS_DP license" (p. 5-6), "Domain Partitioning Management" (p. 1-11), and the "Domain Administration user task" (p. 7-10).

Area and Aggregate Management (View Only) user task

The Area and Aggregate Management (View Only) user task permits users to only view the area and aggregate tree panel.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

The Area and Aggregate Management (View Only) user task is available to the NOC Operator and any user-defined user role profile that has a need for this task.

The Area and Aggregate Management (View Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Connection Management user task

The Connection Management user task permits enterprise network management (ENM) users to provision, view, modify, and delete the physical layer and path layer link topology, and customer bearer services in order to provide a network of layer rate bearer links that support revenue generating customer bearer services and the provisioning of those services in the path layer.

The Connection Management user task also provides users access to the Insert/Remove Node and TDM Line Upgrade tools that can be executed from the management system GUI, rather than from the command line of the server.

Note: If the "Enable ONNS Feature" (p. 6-89) installation parameter is set to be on, users who have the Connection Management user task in their user role profiles can also perform connection management with ONNS-enabled NEs.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Connection Management user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Connection Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Connection Management (View-Only) user task

The Connection Management (View-Only) user task is created for enterprise network management (ENM) users whose role is limited to viewing the physical and path layer link topology.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Connection Management (View-Only) user task is an unassigned task that is available to any user-defined user role profile that has a need for this task.

The Connection Management (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Database Back Up Administration user task

The Database Back Up Administration permits a user to administer database backup schedules.

The Database Back Up Administration user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The Database Back Up Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Database Back Up Administration (View-Only) user task

The Database Back Up Administration (View-Only) user task is created for users whose overall management role contains, or is limited to, the observation of database backup schedules and database backup devices.

The Database Back Up Administration (View-Only) user task is available to any user-defined user role profile.

The Database Back Up Administration (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Domain Administration user task

The Domain Administration user task permits users to create, modify, and delete domains and to assign users and resources to a domain.

Specifically, when the Domain Administration user task is made available in a user's user role profile, that user has the following capabilities:

- They can assign an entire NE to a domain.
- They can activate and suspend domain users. Suspended domain users lose their login privileges, but they remain assigned to the domain until they are explicitly removed.
- They can provision links and connections that fully reside in their network.
- They can create, modify, delete, and deactivate NEs and Network Communications Groups for NEs in their domain.
- They can create customers who belong to their domains.

When the Domain Administration user task is made available in a user's user profile, that user has filtered and/or restricted views of the following:

- The Network Map limits the display of NEs to those NEs that belong to the user's domain.
- Alarm counters and TCA counters are specific to events that have occurred in the user's domain.
- Alarms are specific to the events that have occurred in the user's domain.

- The Alarm log, the NE Command and Response Log, and the NE Notification log are limited to the logging events that have occurred in the user's domain.
- Tools—such as database synchronization, scheduled tasks, and TL1 Macro files—limit the list of NEs to only those NE that reside in the user's domain.
- Network Element functions—such as downloading software, viewing equipment, or creating/modifying/deleting management system entities/objects—are limited to those entities/objects that reside in the user's domain.

The Domain Administration user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task. The Domain Administration user task is the default task that is assigned to the NOC Expert Operator (who can be either a global domain user or specific domain user), and this task can be part of any user-defined user role profile. When a user is assigned to one or more specific domain(s), the "Area and Aggregate Management user task" (p. 7-8) and the "Global UI Settings user task" (p. 7-14) are no longer available to that user.

The Domain Administration user task is only available if the "OMS_DP license" (p. 5-6) is currently installed on the management system. For more information, refer to "OMS_DP license" (p. 5-6) and "Domain Partitioning Management" (p. 1-11).

Ethernet Administration user task

The Ethernet Administration user task permits users to perform Ethernet related administration functions, such as resynchronization and management of the customer list. In addition, users can view the Virtual Switches page.

The Ethernet Administration user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The Ethernet Administration user task is only available if the "OMS_EM license" (p. 5-7) is currently installed on the management system.

Ethernet Element Management user task

The Ethernet Element Management user task permits users to perform Ethernet Element Level Management (EML) related functions and to view the Virtual Switches page. Specifically, this task provides the user with IGMP snooping, MAC table management, and service route management capabilities.

The Ethernet Element Management user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Ethernet Element Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Ethernet Element Management (View-Only) user task

The Ethernet Element Management (View-Only) user task permits users to view Ethernet Element Level Management (EML) related functions and to view the Virtual Switches page. Specifically, this task enables the user to view IGMP snooping, MAC table management, and service route management parameter settings.

The Ethernet Element Management (View-Only) user task is available to any user-defined user role profile that has a need for this task.

The Ethernet Element Management (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Ethernet Hub-and-Spoke Service Provisioning user task

The Ethernet Switched Service Provisioning user task permits users to provision the management system for Ethernet hub-and-spoke service only. In addition, it enables access to the following:

- Ethernet quality-of-service profiles
- Link Aggregation Groups, if the particular NE circuit pack supports Link Aggregation Groups (LAGs); see the *OMS Ethernet Management Guide* for details.
- Domain Partitioning and the Domains list, if Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed.

The Ethernet Hub-and-Spoke Service Provisioning user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Ethernet Hub-and-Spoke Service Provisioning user task is only available if the "OMS_EM license" (p. 5-7) is currently installed on the management system.

Ethernet Infrastructure Provisioning user task

The Ethernet Infrastructure Provisioning user task permits users to provision virtual switch networks (VSNs) and to manage spanning trees. In addition, it enables access to the following:

- Ethernet quality-of-service profiles
- Link Aggregation Groups, if the particular NE circuit pack supports Link Aggregation Groups (LAGs); see the *OMS Ethernet Management Guide* for details.
- Domain Partitioning and the Domains list, if Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed.

The Ethernet Infrastructure Provisioning user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Ethernet Infrastructure Provisioning user task is only available if the "OMS_EM license" (p. 5-7) is currently installed on the management system.

Ethernet Non-Switched Service Provisioning user task

The Ethernet Non-Switched Service Provisioning user task permits users to provision the management system for Ethernet non-switched service only. See the *OMS Ethernet Management Guide* for details.

In addition the Ethernet Non-Switched Service Provisioning user task permits access to the following:

- If the particular NE circuit pack supports Link Aggregation Groups (LAGs), the Link Aggregation Groups icon is enabled. See the *OMS Ethernet Management Guide* for details.
- If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

The Ethernet Non-Switched Service Provisioning user task is only available if the "OMS_EM license" (p. 5-7) is currently installed on the management system.

Ethernet Switched Service Provisioning user task

The Ethernet Switched Service Provisioning user task permits users to provision the management system for Ethernet switched service. In addition, it enables access to the following:

- Spanning trees
- Ethernet quality-of-service profiles
- Link Aggregation Groups, if the particular NE circuit pack supports Link Aggregation Groups (LAGs); see the *OMS Ethernet Management Guide* for details.
- Domain Partitioning and the Domains list, if the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed.

The Ethernet Switched Service Provisioning user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Ethernet Switched Service Provisioning user task is only available if the "OMS_EM license" (p. 5-7) is currently installed on the management system.

Ethernet (View-Only) user task

The Ethernet (View-Only) user task is created for users whose overall management role contains, or is limited to, the observation of the Ethernet connections, virtual switches, and ports lists at the Network Level Management (NML) level only. See the *OMS Ethernet Management Guide* for details.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

The Ethernet (View-Only) user task is an unassigned task that is available to any user-defined user role profile that has a need for this task.

The Ethernet (View-Only) user task is only available if the "OMS_EM license" (p. 5-7) license is currently installed on the management system.

Fault Management Logs Administration user task

The Fault Management Logs Administration user task permits users to view and manage the Alarm Log.

The Fault Management Logs Administration user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The Fault Management Logs Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Global UI Settings user task

The Global UI Settings user task permits users to set up certain system-wide user interface (UI) settings such as saving the node location on the Network Map and customizing system-wide color preferences on the User Preferences page.

The Global UI Settings user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task. The Global UI Settings user task is not available to Domain users; that is, a user who is assigned to one or more domains other than the global domain. For more information about Domain Partitioning Management, refer to "Domain Partitioning Management" (p. 1-11) and the "Domain Administration user task" (p. 7-10).

The Global UI Settings user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Login Session Administration user task

The Login Session Administration user task permits users to disable their own login session if software hang ups or bugs occur. Because the management system does not allow a user to have multiple active login sessions simultaneously, it outputs an error message to the user indicating that an active login session currently exists and offers the user the option of terminating the previous login session. If the user terminates the previous session, the previous login session is terminated for that user only, and that user can log in again with appropriate authentication as in the standard process.

The Login Session Administration user task is available to the NOC Administrator, NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Login Session Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

My Preferences user task

The My Preferences user task permits users to customize the management system application to their preferences, which includes My Network Preferences, Map Preferences, Application Preferences, and Personal Color Preferences.

Note that users can add their own map backgrounds during installation in addition to the map backgrounds that the management system provides. Users can view the entire list of available map backgrounds on the User Preferences page including the map backgrounds that are provided by the management system and the map backgrounds that are added during installation. Refer to the *OMS Getting Started Guide* for details.

The My Preferences user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The My Preferences user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Engineering user task

The NE Engineering user task is intended for users whose overall management role contains, or is limited to, the provisioning and observation of the network element (NE) resources. The NE Engineering user task permits users full access to the Equipment, Ports, Command/Response Log, NE Notification Log, Submap List, and Protection Switch Events (PSEs) pages. It permits users limited access to the NE Management List, Database Synchronization, and Network Map pages and it permits users to only view the Alarm List, the Alarm Log, and the NE/Port Assignment List.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The NE Engineering user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The NE Engineering user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Engineering (View-Only) user task

The NE Engineering (View-Only) user task is intended for users whose overall management role contains, or is limited to, the observation of the network element (NE) resources.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The NE Engineering (View-Only) user task is available to the any user-defined user role profile that has a need for this task.

The NE Engineering (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Management Access user task

The NE Management Access user task enables users whose overall management role contains, or is limited to, the provisioning and observation of the network element (NE) part of the management network. It permits users to do the following:

- Add or remove managed NEs to the management network, which brings the transport resources of these NEs under the control of the OSS
- View a list of managed NEs
- View or modify the management details of any managed NE
- View and manage to the NE-OS connections and the DCN subnets that are created by adding NEs
- View and manage the NE configuration database
- Add or delete unmanaged NEs to the transport topology
- View or modify any unmanaged NEs

In addition, to modify the SHDSL device password, this user task must be combine with the "SHDSL Device Password Modification user task" (p. 7-21).

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

The NE Management Access user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The NE Management Access user task is only available if the "OMS_CORE license" (p. 5-5)is currently installed on the management system.

NE Management user task

The NE Management user task permits enterprise network management (ENM) users to do the following:

- Add or remove *managed* network elements (NEs) to the management network; hence, enabling them to bring the transport resources of these NEs under the OSS control
- View a list of managed NEs and modify the management details of any managed NE
- View and manage the NE-OS connections and DCN subnets created by adding NEs, and view and manage the NE configuration database
- Add or delete *unmanaged* NEs to the transport topology and modify these unmanaged NEs

The NE Management user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The NE Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Management (View-Only) user task

The NE Management (View-Only) user task is intended for users whose topology observation role contains/is limited to the NE part of the management network. The NE Management (View-Only) user task permits users to list and view the details of the managed or unmanaged NEs that are present in the network, to list and view the status of the NE-OS connections and DCN subnets, and to view the status of the NE configuration database synchronization.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

The NE Management (View-Only) user task is an unassigned task that is available to any user-defined user role profile that has a need for this task.

The NE Management (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Software Management user task

The NE Software Management user task is intended for users whose overall management role contains, or is limited to, the upgrade and observation of network element (NE) software. The NE Software Management user task allows users full access to NE Software, NE Notification Logs, and the Scheduler (from the Software submenu) pages.

The NE Software Management user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The NE Software Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

NE Software Management (View-Only) user task

The NE Software Management (View-Only) user task is intended for users whose overall management role contains, or is limited to, the observation of the network element (NE) software.

The NE Software Management (View-Only) user task is an unassigned task that is available to any user-defined user role profile that has a need for this task.

The NE Software Management (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

OMS ASAP Management user task

The OMS ASAP Management user task, which is for the OMS alarm severity assignment profile (ASAP), permits users to access to the NE Profile Templates page of the management system.

The OMS ASAP Management user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The OMS ASAP Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Own Administration user task

The Own Administration user task permits users to administer their password and their regional preferences including Locale, Time Zone, and Date Format.

The Own Administration user task is available to the NOC Administrator, NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Own Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Own TL1 Macro Files Management user task

The Own TL1 Macro Files Management user task enables users to view all TL1 Macro Files, but only to modify or delete their own macro files.

The Own TL1 Macro Files Management user task is available to the NOC Operator and any user-defined user role profile that has a need for this task.

The Own TL1 Macro Files Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Own User Activity Log user task

The Own User Activity Log user task permits users to view only their own User Activity Log.

The Own User Activity Log user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Own User Activity Log user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Performance Monitoring user task

The Performance Monitoring user task permits users to start/stop performance monitoring (PM), and to view PM data, including Protection Switch Events (PSEs).

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Performance Monitoring user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The Performance Monitoring user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Performance Monitoring (View-Only) user task

The Performance Monitoring (View-Only) user task is intended for users whose overall management role contains, or is limited to, the observation of the performance monitoring (PM) data.

If the Domain Partitioning license ("OMS_DP license" (p. 5-6)) is installed, the use of the Domain Partitioning icon and the search and view capabilities for the Domains list is permitted.

If the Root Cause Failure license ("OMS_RCF license" (p. 5-14)) is installed, the use of the Root Cause Failure (RCF) icon and the search and view capabilities for the RCFs is permitted.

The Performance Monitoring (View-Only) user task is available to the to the NOC Administrator, NOC Expert Operator, and NOC Operator and any user-defined user role profile that has a need for this task.

The Performance Monitoring (View-Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Preplan Management user task

The Preplan Management user task permits users to manage (view, add, delete, modify, and execute) the Preplan Restoration function. In general, the Preplan Management user task permits users full use of the management system with the exception of NE Management, Database Synchronization, Alarm List, Alarm Log, Domain Partitioning, and the Domains list where restrictions are imposed. In addition, search and view only capabilities are imposed on Root Cause Failures, Threshold Crossing Alerts, Protection Switch Events, Performance Measurements, and Performance Measurements Points. Refer also to the "Preplan Management (View Only) user task" (p. 7-20).

The Profile Management user task is available to the NOC Expert Operator, NOC Operator, and any user-defined user role profile that has a need for this task.

The Profile Management user task is only available if the "OMS_PREPLAN license" (p. 5-13) is currently installed on the management system.

For additional related information to the Preplan Restoration feature, refer to the "Automatic Routing of Preplan Restoration Connections" (p. 6-161) and "Alarm Triggered Preplan Restoration" (p. 6-160) installation parameters.

Preplan Management (View Only) user task

The Preplan Management (View Only) user task permits users to view the Preplan Restoration function. In general, the Preplan Management user task permits users full use of the viewing and the searching of the management system with the exception of NE Management, Database Synchronization, Alarm List, Alarm Log, Domain Partitioning, and the Domains list where additional restrictions are imposed. In addition, search and view only capabilities are imposed on Root Cause Failures, Threshold Crossing Alerts, Protection Switch Events, Performance Measurements, and Performance Measurements Points. Refer also to the "Preplan Management user task" (p. 7-20).

The Profile Management user task is an unassigned task that is available to any user-defined user role profile that has a need for this task.

The Profile Management user task is only available if the "OMS_PREPLAN license" (p. 5-13) is currently installed on the management system.

For additional related information to the Preplan Restoration feature, refer to the "Automatic Routing of Preplan Restoration Connections" (p. 6-161) and "Alarm Triggered Preplan Restoration" (p. 6-160) installation parameters.

Profile Management user task

The Profile Management user task permits users to manage NE Profile Templates, NE Profiles, NE Profile Assignments, and Ethernet QoS Profiles.

The Profile Management user task is available to the NOC Expert Operator and any user-defined user role profile that has a need for this task.

The Profile Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Profile Management (View Only) user task

The Profile Management (View Only) user task permits users to view NE Profile Templates, NE Profiles, NE Profile Assignments, and Ethernet QoS Profiles.

The Profile Management (View Only) user task is available to the NOC Operator and any user-defined user role profile that has a need for this task.

The Profile Management (View Only) user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

Security Log user task

The Security Log user task permits users to view the Security Log.

The Security Log user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The Security Log user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

SHDSL Device Password Modification user task

The SHDSL Device Password Modification user task permits users to modify the SHDSL device password through the Command Center. This task must be combined with the "NE Management Access user task" (p. 7-16) task so users can access the Command Center.

The Profile Management user task is available to any user-defined user role profile that has a need for this task.

The Profile Management user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

System Administration user task

The System Administration user task permits users to administer application licenses and licensed applications during run time. In addition, this task enables the user to set up preferences for the Network Event Summary page.

The System Administration user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The System Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

System Alarm Supervision user task

The System Alarm Supervision user task permits users to manage the system alarms.

The System Alarm Supervision user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The System Alarm Supervision user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

TMF Session Administration user task

The TMF Session Administration user task enables users to turn the TMF814 Northbound Interface on and off via the management system. For additional details regarding the TMF814 Northbound Interface, refer to Chapter 18, "TMF814 Northbound Interface".

The TMF Session Administration user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The TMF Session Administration user task is only available if the "OMS_TMF license" (p. 5-15) is currently installed on the management system. For additional details, refer to "Available Licenses" (p. 5-4).

User Administration user task

The User Administration user task permits users to administer user accounts and user role profiles.

The User Administration user task is available to the NOC Administrator and any user-defined user role profile that has a need for this task.

The User Administration user task is only available if the "OMS_CORE license" (p. 5-5) is currently installed on the management system.

View a List of User Role Profiles

When to use

Use this task to view a list of user role profiles, which includes all factory-defined user role profiles and user-defined user role profiles.

Related information

See the following topics in this document:

- "User-Defined User Role Profiles" (p. 7-5)
- "User Tasks" (p. 7-7)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view a user role profile.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Role Profiles** icon.

Result: The User Role Profiles page is displayed, which includes all factory-defined user role profiles and user-defined user role profiles.

END OF STEPS

Copy a User Role Profile

When to use

Use this task to copy a user role profile. A factory-defined user role profile or a user-defined user role profile can be copied.

Related information

See the following topics in this document:

- "Factory-Defined User Role Profiles" (p. 7-3)
- "User-Defined User Role Profiles" (p. 7-5)
- "User Tasks" (p. 7-7)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to copy a user role profile.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Role Profiles** icon.

Result: The User Role Profiles page is displayed.

3 On the row of the profile to be copied, click the radio button that appears to the left of the profile name and then click **Copy**.

Result: The User Role Profile page is displayed with the information of the initial profile. Note that if you are copying a factory-defined user role profile, the Profile type now appears as `User defined`.

4 Change the fields as necessary, and then click on **Submit**.

Result: The message `Operation completed successfully` is displayed.

END OF STEPS

Add a User-Defined User Role Profile

When to use

Use this task to add a user-defined user role profile.

Related information

See the following topics in this document:

- "User Role Profile Concepts" (p. 7-2)
- "User-Defined User Role Profiles" (p. 7-5)
- "User Tasks" (p. 7-7)

Before you begin

Become familiar with the user tasks that can be assigned to a user-defined user role profile. These tasks are explained in detail in the "User Tasks" (p. 7-7) section.

If a user account is to have a user-defined user role profile, the user defined profile should be created before the user account is added to the system. If the user account is to have a factory-defined user role profile, the appropriate factory-defined user role profile can be assigned when the user account is created (added). (See"Factory-Defined User Role Profiles" (p. 7-3).)

Task

Complete the following steps to add a user-defined user role profile.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Role Profiles** icon.

Result: The User Role Profiles page is displayed.

3 Click the **New** button.

Result: The Add User Role Profile page is displayed.

4 In the **User Role details** area of the page, complete the **Profile name** field. Refer to "User-defined user role profile nomenclature" (p. 7-6) for details. (Note that the `Profile type: User defined` is displayed on the page.)

5 In the **User Role tasks** area of the page, highlight one or more tasks from the **Available** list and click the right arrow button to move the tasks to the **Selected** list.

6 Click the **Submit** button.

Result: The message `Operation completed successfully` is displayed.

7 To display the new user role profile, click the **User Role Profiles** link at the top left corner of the page.

Result: The new user role profile is displayed.

END OF STEPS

Modify a User-Defined User Role Profile

When to use

Use this task to modify a user-defined user role profile.

Related information

See the following topics in this document:

- "User-Defined User Role Profiles" (p. 7-5)
- "User Tasks" (p. 7-7)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to modify a user-defined user role profile.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Role Profiles** icon.

Result: The User Role Profiles page is displayed.

3 The **Profile Name** column of the table lists the names of the user-defined user role profiles. The name of each user-defined user role profile is a hyperlink.

Click the name of the user-defined user role profile you want to modify.

Result: The selected user role profile is displayed.

4 Highlight one or more tasks from the **Selected** list and move them to the **Available** list, then click the **Submit** button.

Result: The message `Operation completed successfully` is displayed.

END OF STEPS

Delete a User-Defined User Role Profile

When to use

Use this task to delete a user-defined user role profile.

Related information

See the following topics in this document:

- "User-Defined User Role Profiles" (p. 7-5)

Before you begin

A user-defined user role profile cannot be deleted if any user is assigned to that profile.

Remember that factory-defined user role profiles cannot be deleted.

Task

Complete the following steps to delete a user-defined user role profile.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Role Profiles** icon.

Result: The User Role Profiles page is displayed.

3 On the row containing the user-defined user role profile to be deleted, click the button and then click on **Delete**.

Result: A confirmation message asks the following:

`Are you sure you want to delete <profile name>?.`

4 Click the **Yes** button.

Result: An `Operation completed Successfully` message is displayed.

5 To clear the deleted entry from the page, click the **Refresh** button.

Result: The User Role Profiles page is re-displayed without the entry.

END OF STEPS

8 User Accounts

Overview

Purpose

This section contains the conceptual information and the tasks associated with user accounts.

Contents

User Accounts Concepts

Local and remote administration and authentication of user accounts

OMS supports local and remote authentication of user login depending on the type of user accounts being created, the configuration of the OMS host, and the configuration of the remote authentication host (if applicable).

OMS supports the following types of local and remote authentications.

- OMS supports one type of local authentication:
  - **LDAP Authentication**
- OMS supports two types of remote authentications:
  - **Two-Factor Remote Authentication** (also referred to as **RSA Authentication**)
  - **RADIUS Authentication**
- Locally authenticated user accounts are created and administered directly at OMS and independently at each OMS host. These user logins are authenticated locally by the OMS host to which the user attempts to login. The login password is authenticated against the password specified when the account is created.
- Remotely authenticated user accounts are initially created at the remote **authentication server**, and later are automatically created at multiple OMS hosts upon the first successful login to each of these OMS hosts. It is not required to add user accounts to each OMS host directly. Thus the user accounts are centrally administered at the authentication server. When adding user accounts to the authentication server, it is required to specify the OMS hosts to which each of the users is allowed to login. These authorized hosts are referred as the **authentication clients** associated with the remote server. The server only processes the authentication requests coming from its authorized clients. Attempts to login to unauthorized OMS hosts are denied. Each OMS host could be configured to communicate with up to four RADIUS authentication servers. These servers are replicated to backup each other when one goes down. They also take turns to provide services so the work load is balanced.

Types of user accounts

OMS supports the following types of user accounts:

- **LDAP user accounts**
  These accounts are created at a OMS GUI; they are administered by that OMS; they are authenticated by that OMS; the account information is stored in that OMS and managed by the Lightweight Directory Access Protocol (LDAP) software running on that OMS..
- **RSA user accounts**
  These accounts are created and administered by a remote RSA server. After the user accounts are created at the RSA server, users are allowed to log in to multiple OMS hosts for which the RSA server is configured to provide authentication services. The passcode is dynamically updated and users obtain the dynamic passcodes from their **security tokens**. The accounts are automatically created on these OMS hosts upon the first successful login to these hosts. All user account attributes except the passcode are stored in the OMS hosts. Besides the username and the passcode, all attributes are initially set to the default values. Changes to these attributes, except for username and passcode, are possible, and are administered via the factory-created **adminusr** user.
- **RADIUS user accounts**
  These accounts are created and administered by a remote RADIUS server running the Windows-based **Steel-Belted RADIUS** software. User names and passwords are mandatory attributes being added to the RADIUS server. User domains and user role profiles are optional attributes. After the user accounts are created on the RADIUS server, users are allowed to log in to multiple OMS hosts for which the RADIUS server is configure to provide the authentication service. When a user logs in to OMS, the server first verifies the **shared secret key** between the OMS and the server, then it verifies the user password. Only when the shared secret key and the password are verified can the user successfully login. Upon the first successful login, the user account is automatically added to OMS with the user domain attribute and the user role profile attribute populated from the server to OMS. If omitted, these two attributes default to **Global Domain** and **NOC Operator**, respectively.

Data of user accounts

The main components of user accounts are the following.

- **User name**: User identifiers (user IDs), which are also referred to as user names or user logins, are an important mechanism that the management system uses to identify its users and to secure its data.
  For more details on user IDs, refer to "User ID Rules" (p. 8-9).
- **Password/Passcode**: User password/passcode is another important mechanism. Only when the password/passcode is successfully authenticated can the user log in to OMS.
  For more details on Password rules, refer to "Password Rules" (p. 8-11).
- **Domain (Global/Restricted)**

The following apply to global and/or restricted domains:

- For LDAP users, domains are stored in the OMS database and are administered by OMS.
- RSA users are initially created in the global domain and this domain can be changed in the OMS GUI. Refer to the *Modify a Domain* task, which is documented in the *OMS Network Element Management Guide*, for details.

  Note: Initially, RSA users are created in the domain that is defaulted to in "Default User Domain" (p. 6-154) installation parameter, which is the global domain. Users should ensure that the correct domain is set before their first login so the RSA accounts are initially created in the correct domain and to avoid future modifications of the assigned domains.
- For RADIUS users, domains can be stored in the Steel-Belted RADIUS server and populated to OMS at the first successful login to OMS. Users can choose not to store the domain in the Steel-Belted RADIUS server and let OMS default to **Global**. A change of domain is possible and can be done on the Steel-Belted RADIUS server, but the user account must be deleted from OMS and recreated at the next log in to OMS.

- **User Role Profile**

  The following apply to user role profiles:

  - For LDAP users, user role profiles are stored in the OMS database and are administered by OMS.
  - For RSA users, user role profiles are stored in the OMS database and are administered by OMS. RSA users are created with **NOC Operator** initially and can be changed by **adminusr** via the OMS GUI.
  - For RADIUS users, user role profiles can be stored in Steel-Belted RADIUS server and populated to OMS at the first successful login to OMS. Users can choose not to store the user role profile in the Steel-Belted RADIUS server and let OMS default to **NOC Operator**. A change of the user role profile must be done on the Steel-Belted RADIUS server and it is automatically updated to OMS at the next login to OMS.

- **Account status**

  The status of a user account can be *normal* or *suspended*. To achieve one of these states, the management system affords the system administrator with the following actions from the **Go** menu:

  - *Activate User* is the default state for a user account. In this state, the status of the user account *normal*.
  - *Suspend User* is used to temporarily stop the user from accessing the user account. The *suspended* state remains in effect until the system administrator activates the account or chooses to delete the account. In this state, the status of the user account is *suspended*.

  When a user has made more than three consecutive login attempts, the status of that user account becomes *locked out*. Refer to "Invalid login attempts" (p. 8-10) for details.

Important! The factory-defined **adminusr** account that is created for the NOC Administrator cannot be changed. The adminusr account cannot be suspended or deleted. The locked out threshold of three consecutive invalid login attempts does not apply to the **adminusr** account. In addition, the status of Suspend User, Delete User, and Activate User Go menu items do not apply to the **adminusr** account. Only the password of the **adminusr** account can be changed.
Note: RSA/RADIUS user accounts should always be **activated**. If these accounts are ever suspended, they revert to **normal** at the next successful login.

- **Login status**

  OMS maintains and reports the current login/session status for each user, which is the current number of active login sessions.

  – OMS restricts the number of simultaneous login sessions to a single GUI session; therefore, any additional login attempts are denied when a current session is active on either local or remote authentication.

  – OMS allows simultaneous login sessions for Northbound Interface (NBI) users. It also allows login sessions for NBIs when a GUI session is active for a login.

- **GUI user details**

  User details includes personal data such as the user's address and phone numbers, which is stored only in OMS and maintained by OMS. This data is irrelevant to remote authentication and is not stored in the remote servers.

Security warnings displayed to users

Because the management system uses the HTTPS/SSL protocol, security warnings are displayed to users upon their login into the management system. Users can select **Yes** to proceed and **Grant** or **Grant Always** to disable some of the warnings. To disable all of the warnings, follow the steps in the “Eliminate Security Warnings upon User Login” (p. 8-25) task.

Common User Account Features

Forced logout

OMS supports a concept known as *single sign-on*. Each user can have one login session on OMS at a time. Any attempt to log in a second time before logging out of the previous session is rejected with an option of a force-logout of the previous session.

Password aging/ Password expiration/ Password Alarm

Password aging, password expiration, and password alarm are value-added security features that are applicable to LDAP user accounts on OMS, but not to RSA/RADIUS user accounts.

For more details on password rules, refer to “Password Rules” (p. 8-11).

Remote Authenticated User Account Features

Two-Factor (RSA) remote authentication

When the OMS management system is configured to use Two-Factor (RSA) authentication method, the following apply:

- Login from OMS GUI is authenticated by the remote RSA authentication server.
- Any login from the northbound interface (NBI) is not authenticated by the remote RSA authentication server. Users should configure OMS to also allow the local LDAP authentication method for this purpose. For more details, refer to "Enable/Disable Authentication Method" (p. 8-26).
- Before logging in to OMS, the RSA server must be configured to include the user accounts that specify to which OMS hosts (IP addresses) these users are permitted to login.
- Users must have a security token that provides the passcode for login. Users cannot set or change the passcode values.
- All other account attributes, such as Account Status and Login Status, are stored in OMS and maintained by OMS. Changes of these attributes are done at OMS directly.
- Attributes of User Domain and User Role Profile are also stored in OMS and maintained by OMS. Initially, they are set to **Global** and **NOC Operator**, respectively, when the accounts are added to OMS upon the first successful login. After that, changes can be done at OMS through the OMS GUI.
- **Configurations**: Both the RSA server an the OMS hosts require proper configuration. For more details, refer to "Enable/Disable Authentication Method" (p. 8-26) and "Configure Two-Factor Remote Server" (p. 8-28).

RADIUS remote authentication

The following apply to RADIUS remote authentication:

- **Login Access**

  Login from the following sources could be authenticated by the RADIUS server:

  – OMS GUI

  – TMF NBI

  – MTOSI (XML) interface
- **Configuration**

  Both the RADIUS server and the OMS hosts require proper configuration. For more details, refer to "Enable/Disable Authentication Method" (p. 8-26) and "Configure a Steel-Belted RADIUS Server " (p. 8-30).

- **Authentication Protocol**
  OMS functions as a Network Access Server (NAS), or a RADIUS Client. It routes the user login password to the remote RADIUS server for authentication through the Password Authentication Protocol (PAP). OMS encrypts the password before sending it and the RADIUS server decrypts it after receiving it.
- **Multiple remote RADIUS servers**
  The system supports multiple RADIUS servers with replicated data for added reliability and/or load sharing. OMS dispatches authentication requests according the following configurable options:
  - **Sequential** use of the remote RADIUS servers where the priority for using the server corresponds to the server number. The lower that the number is; the higher that the priority is. For example: server 1 has the highest priority; server 4 has the lowest priority.
  - **Round-Robin** use of the remote RADIUS servers where the first priority is to use the next server in the sequence. The round-robin option balances the load among the servers.

  With either option, if the highest priority server becomes unavailable, the next server in the sequence is given the highest priority.

  Example
  A OMS is configured to communicate with 4 RADIUS servers, where numbers 2 and 4 are up; numbers 1 and 3 are down. The last access was authenticated by server 2. If the **SEQ** option is chosen, server 2 has the highest priority for every future access request. If the **Round-Robin** option is chosen, then server 4 has the highest priority for the next access request; next time server 2 has the highest priority; after that the two available servers are rotated to have the highest priority.

Enable/ Disable authentication method on OMS

When a remote authentication method is desired, not only the remote authentication server but also OMS must be configured to enable the selected method. While a remote authentication method is enabled, OMS might not need to enable the local authentication at the same time.

When the RSA authentication is chosen, the newly added user accounts default to the **NOC Operator** user role profile and the **Global** domain. To change the user role profile and/or the domain partition of these accounts, users must login to **adminusr**, the only factory-created LDAP user account, to make the changes directly on OMS. In this case, users must enable the local authentication.

When the RADIUS authentication is selected, the newly added user accounts will have the user role profile and the domain partition as those being pre-provisioned on the remote authentication. Users need not login to **adminusr** to change the role profile and/or domain. In this case, users should disable the local authentication.

When the remote server becomes unavailable, the corresponding remote user accounts are not operational. To continue access to the OMS GUI, users should enable the local authentication.

See "Enable/Disable Authentication Method" (p. 8-26) for the step-by-step procedure.

Automatic creation of user account

When a user is successfully authenticated by a remote security server, but does not have an existing account for that user name in the system, OMS automatically creates that account. It uses information from the authentication message and default values.

For more details on adding a user account, refer to "Add a User Account" (p. 8-15).

Logs

When a user attempts to access the system, OMS enters a record in the Security Log with the following information:

- successful or denied
- authenticated locally or by a remote server

When a user account is created or modified on OMS, the system enters a record in the Security Log to identify who performed the account. This record indicates if the system itself performed this action as a result of an authentication message from a remote security server.

Modify remote user accounts data

Administrators cannot change the following account data on OMS directly when they modify the user account.

- User name

Administrators can modify the following account data on OMS directly and the changes take effect immediately:

- Account status
- Login status (by login/logout)
- GUI user information
- Domain and User Role Profile for RSA user

Administrators can modify the following account data in three steps:

- **For RADIUS accounts**: Password, User Domain
- **For RSA accounts**: Passcode information
    1. Delete the user account from OMS
    2. Make changes on the remote server
    3. Login to OMS to recreate the user account on OMS

Administrators can modify the following account data on the remote server, the data is automatically updated on OMS upon the next login to OMS:

- User Profile of RADIUS account

Delete remote user accounts

Complete the following steps to delete a user account:

1. Delete the user account from OMS.
2. Delete the user account from the remote server.

Fore more details on how to delete a user account from OMS, refer to "Delete a User Account" (p. 8-19).

User ID Rules

Purpose

User identifiers (user IDs), which are also referred to as *user names* or *user logins*, are an important mechanism that the management system uses to identify its users and to secure its data. Along with user passwords and the user role profile, user IDs are a significant component of a user account.

Rules

The following rules apply to selecting user IDs:

1. A user ID must be unique.
2. A user ID can have 7 to 10 characters.

   The following installation parameters govern the initial values that are set for the minimum and maximum character lengths that are allowed for user IDs:

   - "User Name Minimum Length" (p. 6-124)
   - "User Name Maximum Length" (p. 6-125)
3. A user ID must consist of only letters and digits. In addition, it can contain special characters; however, the following special characters are not allowed:
   **“ ' ; { } < > & + . / **
   Specifically, the user ID must contain the letters and digits that appear in the 7-bit, 128-character set defined in Table 5 of the International Reference Alphabet (ITU-T T50).
4. A user ID is case-sensitive; that is, an uppercase letter is considered a different character than its lowercase equivalent, and the correct case of the letter must be entered.

Additional Rules for RSA/RADIUS User ID

While the LDAP user ID must be unique within the belonging Optical Management systems, the RSA/RADIUS user ID must be unique across the network, that is, in all the Optical Management systems, which are authenticated by the same remote server.

RSA/RADIUS user ID follows the same rules of length and characters and case sensitivity as that of LDAP user ID but has no restriction of the pattern.

Invalid login attempts

When a user enters invalid user ID or password, the management system warns:
`You are not authorized to log in.`

When the management system receives three consecutive invalid login attempts, the management system puts the user account into the *locked out* state, issues a system alarm, and enters a record in the Security Log. An error message informs the user that the account was locked out due to invalid log in attempts and that the administrator can restore the status of the account to active.

Proprietary agreement warning message

As an installation option, the management system can be configured to display a proprietary warning message upon a successful user login. The user can accept or decline the proprietary agreement. If the user accepts the agreement, that user gains access to the management system. If the user declines the agreement, that user is logged off of the management system. Refer to "Installation Parameters and the Proprietary Agreement" (p. 6-164), the explanation of the "Proprietary Agreement Warning File" (p. 6-124) and "Proprietary Agreement Warning Message Flag" (p. 6-123) installation parameters, and the "Create a Customized Proprietary Agreement" (p. 6-168) task.

User login inactivity/non-use

The management system automatically times a user out if the user (including the NOC Administrator) has not sent any requests from the management system for a specified period of time. The timeout is governed by an administrator-tunable installation parameter. Refer to the "Session Inactivity Timeout Period" (p. 6-123) and "Session Inactivity Timeout Flag" (p. 6-123) installation parameters for details. Note: If the installation parameters are not specified, the web server session timeout is used.

When a user times out, all opened management system pages are closed and replaced by the Logout page, which displays a message that the particular user is now logged out.

Besides the user login inactivity timeout, the management system also institutes a period of non-use for a user account. The period of non-use is governed by an administrator-tunable installation parameter. The non-use period can range from 1 day to 120 days. The default for the period on non-use is 30 days. Refer to the “Password Period of Non Use” (p. 6-122) installation parameter for details.

Password Rules

Purpose

A user password is the entity that is to be authenticated, either locally by OMS, or remotely by a remote authentication server.

Rules

The following rules apply to selecting passwords:

1. Any administrator-assigned password must be immediately changed when a user first logs in to the system.
2. A password must have a minimum of 8 and a maximum of 20 characters that are letters, numbers, or special characters (symbols). Specifically, the password must contain the letters, digits, and symbols that appear in the 7-bit, 128-character set defined in Table 5 of the International Reference Alphabet (ITU-T T50).

   The following installation parameters govern the initial values that are set for the minimum and maximum character lengths that are allowed for passwords:

   - “User Password Minimum Length” (p. 6-125)
   - “User Password Maximum Length” (p. 6-126)
3. A password must contain at least two uppercase and/or two lowercase letters. Passwords are case-sensitive; that is, an uppercase letter is a different character than its lowercase counterpart, and the correct case of the letter must be entered.
4. A password must contain at least one special character (symbol). The following special characters (symbols) are not allowed:
   ' # $ * / @ < > &
   A space (or a blank character) and a delete are not allowed.
5. A password can begin with any valid character and all alphabetical, numerical, and special characters (symbols) can be randomly positioned.
6. A password must contain at least one Arabic numeral:
   0 1 2 3 4 5 6 7 8 9
7. A password cannot contain a user login name or any reversal or circular variation of the user login name. In this case, the management system treats an uppercase letter and its corresponding lowercase equivalent as identical characters.

8. A new password must differ from the old password by at least three characters. In this case, the management system treats an uppercase letter and its corresponding lowercase equivalent as identical characters.
9. The new password cannot be one of the five most recently used passwords.

Invalid login attempts

Refer to "Invalid login attempts" (p. 8-10), which explains how the management system acts upon invalid user IDs and passwords.

Password aging

The management system supports password aging, which enables the system administrator to specify a particular time period in which a password is allowed to remain active and usable. Refer to the "Password Aging Time" (p. 6-121) installation parameter for details. Note that the **adminusr** password for the NOC Administrator is also subject to password aging.

The management system also displays an early warning message to notify a user that a password needs to be changed. The system administrator can specify the time period in which the warning message should appear. Refer to the "Password Warning Time" (p. 6-122) installation parameter for details.

Password expiration

After a password has expired, the management system offers the respective user an opportunity to change the password when the user logs in with the expired password. The management system prompts the user with the following message:

```
Your password is already expired. Please change it to a new one.
```

Password-related platform alarms

The following hot link provides additional information on a platform alarm that could be related to the malfunctioning of a password: "INVALID_PASSWD_DETECTED" (p. 42-18).

Exception for RSA passcode and RADIUS password

The following are the exception for the RAS passcode and RADIUS password:

- The password can only be changed on remote server.
- The term **passcode** applies to RSA user account and **password** applies to RADIUS user account.
- The password is not restricted to at least two uppercase and/or two lowercase letter, at one Arabic numeral

- The password can contain a user login name or any reversal or circular variation of the user login name.
- The new password need not differ from the old password by at least three characters, and can be a recently used password.
- The password aging, password expiration, and password-related platform alarms do not apply to RSA/RADIUS passwords.

View a List of User Accounts

When to use

Use this task to view a list of user accounts.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view a list of user accounts.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click **User Accounts**.

Result: The User Accounts page is displayed, which lists all user accounts along with pertinent user account information.

END OF STEPS

Add a User Account

When to use

Use this task to add a user account.

Related information

See the following topics in this document:

- "User Role Profile Concepts" (p. 7-2)
- "Factory-Defined User Role Profiles" (p. 7-3)
- "User-Defined User Role Profiles" (p. 7-5)
- "Add a User-Defined User Role Profile" (p. 7-25)
- "User ID Rules" (p. 8-9)
- "Password Rules" (p. 8-11)

Before you begin

If you plan to assign a user-defined user role profile and not a factory-defined user role profile to the account being added, create the user-defined user role profile first. Refer to "Add a User-Defined User Role Profile" (p. 7-25) for details.

If you plan to assign a factory-defined user role profile to the account, become familiar with the user tasks that can be made available to the account. These tasks are explained in detail in the "User Tasks" (p. 7-7) section.

For domain information, refer to the appropriate domain-related tasks that are documented in the *OMS Network Element Management Guide*.

Task: Add an LDAP user account on the OMS GUI.

Complete the following steps to add a user account.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Accounts** icon.

Result: The User Accounts page is displayed.

3 Click the **New** button.

Result: The Add a User Account page is displayed.

4 In the User access area of the page, complete the **User name**, **Password**, and **Confirm password** fields.

5 In the User Scope area of the page, select the **Domain** and the **User Role Profile** that is to govern the activity of the account.

6 Click the **Submit** button.

Result: The user account is added.

The message `Operation completed successfully` is displayed.

END OF STEPS

Task: Add a RADIUS user account

1 See "Administer RADIUS Authentication" (p. 8-33) for the information required to add a RADIUS user account.

Note: RADIUS user accounts must be added on the RADIUS server, not on OMS.

END OF STEPS

Task: Add an RSA user account

1 See "Configure Two-Factor Remote Server" (p. 8-28) for the information required to add an RSA user account.

Note: RSA user accounts must be added on the RSA server initially, not on OMS.

END OF STEPS

Modify a User Account

When to use

Use this task to modify a user account.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

This task does not have any preconditions.

Task: Modifying an LDAP user account on the OMS GUI

Complete the following steps to modify a user account.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click **User Accounts**.

Result: The User Accounts page is displayed.

3 The **User Name** column of the table lists the names of the user account. The name of the user account is a hyperlink.

Click the name of the user account you want to modify.

Result: The User Account page is displayed.

4 Change the appropriate information on the page, then click the **Submit** button.

Result: The system makes the requested user account modification(s).

The message `Operation completed Successfully` is displayed.

END OF STEPS

Task: Modifying a RADIUS user account

1 See "Modify remote user accounts data" (p. 8-8) for the information required to modify a RADIUS user account.

Note: To modify a RADIUS user account, some data can be modified directly on OMS and other data can be modified only on the RADIUS server.

END OF STEPS

Task: Modifying an RSA user account

1 See "Modify remote user accounts data" (p. 8-8) for the information required to modify an RSA user account.

Note: The passcode of an RSA user account cannot be modified.

END OF STEPS

Delete a User Account

When to use

Use this task to delete a user account.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

Verify that the user to be deleted is not logged in to the management system.

Task: Delete an LDAP user account on the OMS GUI

Complete the following steps to delete an LDAP user account on the OMS GUI.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Accounts** icon.

Result: The User Accounts page is displayed.

3 Click the radio button in the row of the user account to be deleted.

Result: The user account to be deleted is selected.

4 From the Go menu, select **Delete User** and click the **Go** button.

Result: A confirmation dialog box is displayed.

5 Click the **OK** button.

Result: The user account is deleted.

The message `Operation completed successfully` is displayed.

6 To clear the deleted entry from the page, click the **Refresh** button.

Result: The User Accounts page is redisplayed without the entry.

END OF STEPS

Task: Delete an RSA/RADIUS user account

1 See "Delete remote user accounts" (p. 8-9) for the information required to delete a remote user account.

END OF STEPS

Activate a User Account

When to use

Use this task to activate a user account.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

Verify that the account to be activated is in the suspended or locked out state.

Task

Complete the following steps to activate a user account.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Accounts** icon.

Result: The User Accounts page is displayed.

3 Click the radio button in the row of the user to be activated.

Result: The user account to be activated is selected.

4 From the Go menu, select **Activate User** and click the **Go** button.

Result: The user account is activated.

The message `Operation completed successfully` is displayed.

5 Click the refresh button to view the latest changes.

END OF STEPS

Stop a User Session

When to use

Use this task to stop the current login session for a user.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

Verify that the user account to be stopped does not have any jobs pending.

Task

Complete the following steps to stop a user session.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Accounts** icon.

Result: The User Accounts page is displayed.

3 Click the radio button in the row of the user account session to be stopped.

Result: The user account whose session is to be stopped is selected.

4 From the Go menu, select **Stop Session** and click the **Go** button.

Result: The current user account session is stopped.

The message `Operation completed successfully` is displayed.

5 Click the refresh button to view the latest changes.

END OF STEPS

Suspend a User Account

When to use

Use this task to suspend a user account.

Related information

See the following topic in this document:

- "User Accounts Concepts" (p. 8-2)

Before you begin

Verify that the account to be suspended is in the active state.

Realize that once a user account is suspended, the user can no longer log in to the management system.

Rules for RSA/RADIUS user accounts

1 RSA/RADIUS user accounts should remain activated at all time. If for any event any user account becomes suspended, it will be automatically reverted to normal at the next login to OMS.

END OF STEPS

Task

Complete the following steps to suspend a user account.

1 From the Administration home page, select **Users**.

Result: The Users page is displayed.

2 Click the **User Accounts** icon.

Result: The User Accounts page is displayed.

3 Select the account to be suspended.

4 From the Go menu, select **Suspend User** and click the **Go** button.

Result: The user account is suspended, which means that the user can no longer log in to the management system.

The message `Operation completed successfully` is displayed.

5 Click the refresh button to view the latest changes.

END OF STEPS

Eliminate Security Warnings upon User Login

When to use

Use this procedure to eliminate all security warnings that appear when users login into the management system.

Related information

See the following topic in this document:

- "Security warnings displayed to users" (p. 8-5)
- "Security Management" (p. 1-10)

Before you begin

Step 1 of this task requires you to authenticate the security certificate and/or key for your HP® server by an authorized organization. Have the contact information for the authorizing organization (RSA or VeriSign) handy.

Task

Complete the following steps to eliminate all security warnings that appear when users login into the management system.

1 Authenticate the security certificate and/or key for your HP® server that is running the OMS.

2 Replace the following files with your own certificate and key:

For the public key, replace the **server.crt** file that is found in the **/opt/hpws/apache/conf/ssl.crt** directory.

For the private key, replace the **server.key** file that is found in the **/opt/hpws/apache/conf/ssl.kdy** directory.

END OF STEPS

Enable/Disable Authentication Method

When to use

Use this task to **choose** or/and **enable/disable** authentication method.

Related information

See the following topic in this document:

- "Remote Authenticated User Account Features" (p. 8-6)

Before you begin

From the machine on which the management system is running, log in as `oms`.

Task

Use this task to disable local authentication. Enter the following commands on the unix shell:

1 **`cd /opt/lucent/platform/bin`**

`./lt_param_reconfig`

2 Enter **15** to select External Authentication Variables.

3 Enter **1** to select an authentication method.

4 Select one of **STD (Standard)**, **RSA**, or **RADIUS**.

5 Enter **Y** to accept the change.

6 Enter **2** to select Allow local GUI user authentication.

7 Enter **2** to select **YES** or **NO** per users' justification of the need to enabling the local authentication. The general rules for enabling local authentication in parallel with a remote authentication:

- When a remote authentication method is chosen but the remote server become unavailable. This enable the use of local user accounts to operate until the remote server is repaired.
- RSA authentication method is chosen and users need to change the User Role profile or User Domain of a newly created user account. Users will need to login as **adminusr**, a factory-created LDAP account, to make the change.

8 Enter **y** to Accept the change.

9 Enter **q** to exit the lt_param_reconfig program.

10 Enter the following command to restart the GUI subsystem:

```
gui_platform_cntrl restart
```

Result: The change of this system parameter is effective only after the GUI subsystem is restarted.

For more details on Steel-Belted RADIUS Server, refer to "Configure a Steel-Belted RADIUS Server " (p. 8-30) .

END OF STEPS

Configure Two-Factor Remote Server

When to use

Use this task to configure the Two-Factor authentication server, which is also called the RSA server.

Related information

See the following topic in this document:

- "Remote Authenticated User Account Features" (p. 8-6)

Before you begin

Obtain a binary file called **sdconf.rec** from the administrator of the RSA authentication server. This file contains all of the information the management system needs to connect to the remote RSA authentication server.

Task

Complete the following steps to change the system parameters to select the RSA two-factor authentication method.

1 Copy the **sdconf.rec** file to the following directory on the management system:

```
/etc/opt/lucent
```

The owner of this file should be **oms** and the file permission should be **755**.

2 From the machine on which the management system is running, log in as `oms`.

3 Enter the following command lines:

```
cd /opt/lucent/platform/bin
./lt_param_reconfig
```

4 Enter **15** to select External Authentication Variables.

5 Enter **1** to select Authentication method.

6 Enter **3** to select RSA.

7 Enter **y** to Accept the change.

8 Enter **q** to exit the lt_param_reconfig.

9 Enter the following command to restart the GUI subsystem:

```
gui_platform_cntrl restart
```

Result: The change of this system parameter is effective only after the GUI subsystem is restarted.

END OF STEPS

Configure a Steel-Belted RADIUS Server

When to use

Use this task to configure the Steel-Belted RADIUS server for authentication to OMS.

Related information

See the following topic in this document:

- "Remote Authenticated User Account Features" (p. 8-6)

Before you begin

Install the Windows-based Steel-Belted RADIUS server software to your PC at the following location:

C:\Radius

Task

Complete the following steps to configure the Steel-Belted RADIUS server.

1 Obtain the OMS RADIUS attributes dictionary file named **lucentoms.dct** from your OMS host through the following URL:

Https:\\<your host IP address>/RADIUS/lucentoms.dct

Install this file to your PC at the following location:

C:\Radius\Service

2 Add the following to the file **C:\Radius\Service\vendor.ini:**

```
vendor-product = Alcatel-LucentOMS
dictionary = lucentoms
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3 Add the following to the file **C:\Radius\Service\dictiona.dcm** under vendor specific dictionary files:

@lucentoms.dct

4 For debugging, turn on Steel-Belted RADIUS traces by modifying file **C:\Radius\Service\radius.ini** as follows:

LogLevel = 2

TraceLevel = 2

5 The configuration will not take effect until you restart the Steel-Belted RADIUS server as follows:

Click **Start>Settings>Control Panels>Administrative Tools>Services**

Scroll down and select:

Steel-Belted Radius

Right click **start** (or **restart**)

6 Ensure that the corresponding OMS hosts have the **AXLRadius.jar** file installed as specified in the *Optical Management System (OMS) PC Platform Installation Guide* (365-315-163R6.1). To ensure that these hosts are configured properly, use the **/opt/lucent/platform/bin/lt_param_reconfig** tool to set the proper values for the following OMS system parameters:

- Authentication method [RADIUS]
- Allow local GUI user authentication [**NO**| YES] (Select **YES** when the RADIUS server is down.)
- Default user role profile [**NOC Operator**|<type in any profile name>]
- Default user domain type [**Global**|Restricted]
- Authentication server retries [3]
- Authentication server timeout in seconds [30]
- Authentication server selection policy [SEQ]
- Address of external server 1 (enter your Steel-Belted RADIUS server's IP address & port)
- Shared secret for server 1 (enter the secret shared between OMS and Steel-Belted RADIUS)
- Address of external server 2 (IP address & port of your backup Steel-Belted RADIUS server)
- Shared secret for server 2
- Address of external server 3
- Shared secret for server 3
- Address of external server 4

- Shared secret for server 4
- Vendor private enterprise number [1751]
  Note: If the vendor ID is set to a different value, update the "Vendor Private Enterprise Number" (p. 6-160) installation parameter to reflect the new vendor ID value.

END OF STEPS

Administer RADIUS Authentication

When to use

Use this task to administer OMS user accounts on the Steel-Belted RADIUS server.

Related information

See the following topics in this document:

- "Remote Authenticated User Account Features" (p. 8-6)
- "Configure a Steel-Belted RADIUS Server " (p. 8-30)

Before you begin

The Steel-Belted RADIUS server must already be configured. See the "Configure a Steel-Belted RADIUS Server " (p. 8-30) task.

Follow the instructions specified in the *Steel-Belted RADIUS Administration Guide* provided by Juniper, Incorporated. This *Service Provider Edition* can be found at the following path on your PC:

C:\Radius\Docs\admin_gee.pdf

OMS supports the Steel-Belted RADIUS server in the following tasks:

- "Task: Add/Edit/Delete OMS as client to an Steel-Belted RADIUS server" (p. 8-33)
- "Task: Add/Edit/Delete OMS users to an Steel-Belted RADIUS server" (p. 8-34)
- "Task: Add/Edit/Delete profiles" (p. 8-34)
- "Task: Select an authentication policy" (p. 8-35)

Task: Add/Edit/Delete OMS as client to an Steel-Belted RADIUS server

Complete the following steps to add/edit/delete OMS as a client to an Steel-Belted RADIUS server:

1 Complete the following required information as shown. Use the default values for everything else.

Name: <enter your OMS host name>

IP Address: <enter your host OMS IP address>

Shared Secret: <enter the same string specified in the OMS system parameter>

Vendor Make/Model: **Alcatel-LucentOMS**

END OF STEPS

Task: Add/Edit/Delete OMS users to an Steel-Belted RADIUS server

Use this task to add/edit/delete OMS users to an Steel-Belted RADIUS server

1 Complete the following required information as shown. Keep the default values for everything else.

Name: <enter the OMS username> Note: This is always shown as upper case.

Password : <enter the user password as text string>

User profile: <select a suitable OMS user profile that you create in "Task: Add/Edit/Delete profiles" (p. 8-34)>

Return List Atttributes : set the following:

- OMS-User-Domain : select Global or Restricted
- OMS-User-Role-Profile: <type in the profile>
  The following can be used for a OMS user role profile:
  1. NOC Administrator
  2. NOC Expert Operator
  3. NOC Operator
  4. Or any user profile that is added to OMS and is spelled exactly as shown on the OMS GUI

  Check List Attributes (Optional):

  - **Name :** Enter the user name; This user name will be case-sensitive, letter by letter, when it is used to login to OMS. Do not specify this attribute if you want this user name to be case-insensitive (any combination of upper/lower case of letters will be accepted).

END OF STEPS

Task: Add/Edit/Delete profiles

Complete the following steps to add/edit/delete profiles:

1 Complete the following required information as shown below. Keep the default values for everything else.

Steel-Belted RADIUS profiles are not the same as User Role profiles in OMS. If many user accounts must be created, create Steel-Belted RADIUS profiles with the returned data listed in "Task: Add/Edit/Delete OMS users to an Steel-Belted RADIUS server" (p. 8-34).

Examples:

A Steel-Belted RADIUS profile named **GLOBAL_EXPERT** returns to OMS the following:

- OMS-User-Domain=Global
- OMS-User-Role-Profile=NOC Expert Operator

Another Steel-Belted RADIUS profile name **RESTRICT_OPERATOR** returns to OMS the following:

- OMS-User-Domain=Restricted
- OMS-User-Role-Profile=NOC Operator

Note: If you want OMS software to default to the domain and user role profile that is specified in the OMS installation parameters, do not include any Return List Attributes.

END OF STEPS

Task: Select an authentication policy

Complete the following step to select an authentication policy:

1 Select the following policy if it is not already selected:

Native User

END OF STEPS

9 Operations

Overview

Purpose

This chapter contains conceptual information and the related tasks that are needed for the basic operation of the management system.

Contents

Processes

Types of operating processes

To bring up and to bring down the management system successfully, the following two processes must be invoked:

- *Application processes*, which include those processes invoked by all third party software and the management system application itself (**oms**).
- *Web server processes*, which are those processes invoked by the GUI web server (GWS). Refer to "GWSs" (p. 11-9) for details.

The operating processes platform commands

The management system has two different operating processes that started, stopped, and verified with different platform commands:

- The **platform_cntrl start** and **platform_cntrl stop** commands are used to start and stop all application processes, which include third party software and the management system application (**oms**), which is often referred to as the *GUI*. In addition, these commands can also be used to start and stop the GUI web server (GWS), TL network adaptors (TNAs), CMISE network adaptors (CNAs), NMA network adaptors (NMA) and Bulk Performance Monitoring (BPM).
  The state of all application processes can only be verified accurately with a corresponding **platform_cntrl status** command.
  Refer to the "Start the Platform" (p. 9-5) and "Stop the Platform" (p. 9-7) tasks for complete instructions.
- The **gui_platform_cntrl start** and **gui_platform_cntrl stop** commands are only used to start and stop all GUI web server (GWS) processes, which include the Apache (web) server along with all **http** processes. The state of all GUI web server processes can only be verified accurately with a corresponding check for **http** processes, which is done with the **gui_platform_cntrl status** command line. Refer to "GWSs" (p. 11-9) for additional information.

These two sets of commands are needed to start and to stop the entire management system.

Important! Because the **platform_cntrl start** and the **platform_cntrl stop** commands also start and stop the GUI (the OMS management system application), the **gui_platform_cntrl start** and **gui_platform_cntrl stop** commands do not have to be run to bring the management system up or down if the **platform_cntrl start** and the **platform_cntrl stop** commands are run.

hostchange command

The **hostchange** command, which is executed as **root** from the command line of the host device, is used to change the name or the IP address of the host.

The **hostchange** command is supported on the *Server Platform*.

The **hostchange** command is not supported on the *PC Platform*.

Command Format:

hostchange --hostname <newhostname> --ipadddress <newIPaddress>

Where:

newhostname is the new name that is being given to the new host device, which must be less than or equal to eight alphanumeric characters. Note that hostname is preceeded by two dashes, not one dash.

newIPaddress is the new IP address that is being given to the host device. Note that ipaddress is preceeded by two dashes, not one dash.

Refer to the “Change the Name of the Host HP® Server” (p. 9-14) and “Change the IP Address of the Host HP® Server” (p. 9-16) tasks for instructions.

Important! For implications regarding web servers and hostnames in Disaster Recovery configurations, refer to “Disaster Recovery and distributed web server architecture” (p. 20-4).

Check Running Services

When to use

Use this task each day to check running services to determine if all required processes are functioning. Running services, such as daily cron jobs, might get hung after daily backups.

Related information

See the following topic in this document:

- "Processes" (p. 9-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check running services.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command lines to check the status of the management system:

```
platform_cntrl status
```

Result: The command output is similar to the following:

```
Overall System status...[shutdown]
platform...[Down]
oms...[Down]
tna...[Down]
```

3 Enter the following command to check the status of the web server:

```
gui_platform_cntrl status
```

END OF STEPS

Start the Platform

When to use

For non-Serviceguard configurations, use this task to start the management system platform, which includes all applications that are loaded on the server such as the GUI web server (GWS), T1 network adaptors (TNAs), CMISE network adaptors (CNAs), NMA network adaptors (NMA) and Bulk Performance Monitoring (BPM).

Related information

See the following topics in this document:

- "Processes" (p. 9-2)
- "GWSs" (p. 11-9)
- "Stop the Platform" (p. 9-7)

Before you begin

The HP® servers, in which the management system software is loaded, must be up and running.

Task

For non-Serviceguard configurations, complete the following steps to start the management system platform, which includes all applications that are loaded on the server such as the GUI web server (GWS), T1 network adapters (TNAs), CMISE network adapters (CNAs), NMA network adapters (NMA) and Bulk Performance Monitoring (BPM).

1 From the machine on which the management system is running, log in as **oms**.

Result: You are now logged in as **oms**.

2 To determine if any application processes are running, enter the following command line:

```
platform_cntrl status
```

Result: If the system returns the status of `running`, the platform is up.

If the status of `running` is not returned, go to the next step.

3 Start the platform by entering the following command:

```
platform_cntrl start
```

4 From any PC that is designated to run the application, log in to the management system as **`adminusr`**. If you are not familiar with how to log in into the management system, use the steps provided in the "Log in to OMS for the First Time" (p. 3-33) task or refer to the *OMS Getting Started Guide* for details.

END OF STEPS

Stop the Platform

When to use

For non-Serviceguard configurations, use this task to stop the management system platform, which includes all applications that are loaded on the server such as the GUI web server (GWS), T1 network adapters (TNAs), CMISE network adapters (CNAs), NMA network adapter (NMA) and Bulk Performance Monitoring (BPM).

Related information

See the following topics in this document:

- "View a List of User Accounts" (p. 8-14)
- "Processes" (p. 9-2)
- "Start the Platform" (p. 9-5)

Before you begin

Notify all users that the management system platform is coming down and that they must be logged off of the management system.

Task

For non-Serviceguard configurations, complete the following steps to stop the management system platform, which includes all applications that are loaded on the server such as the GUI web server (GWS), T1 network adapters (TNAs), CMISE network adapters (CNAs), NMA network adatper (NMA) and Bulk Performance Monitoring (BPM).

1 From the machine on which the management system is running, log in as **`oms`**.

Result: You are logged in as **`oms`**.

2 Enter the following command to stop the management system platform:

```
platform_cntrl stop
```

Result: The platform is stopped, which includes all applications that are loaded on the server such as the GUI web server (GWS), the T1 network adapters (TNAs), the CMISE network adapters (CNAs), the NMA network adapter (NMA) and Bulk Performance Monitoring (BPM).

3 Enter the following command to verify platform is stopped:

platform_cntrl status

Result: The command output is similar to the following:

```
Overall System status...[shutdown]
platform...[Down]
oms...[Down]
tna...[Down]
bpm...[Down]
```

END OF STEPS

Start the GUI Web Server

When to use

Use this task to start the GUI web server (GWS).

Related information

See the following topics in this document:

- "gui_platform_cntrl command" (p. 11-10)
- "Processes" (p. 9-2)
- "GWSs" (p. 11-9)
- "Stop the Platform" (p. 9-7)

Before you begin

The HP® servers, in which the management system software is loaded, must be up and running.

Read the "gui_platform_cntrl command" (p. 11-10) for details.

Task

Complete the following steps to start the GUI web server (GWS).

1 From the machine on which the management system is running, log in as **oms**.

Result: You are now logged in as **oms**.

2 To determine if any application processes are running, enter the following command line:

```
gui_platform_cntrl status
```

Result: The command output should not display any running processes.

3 Start the GWS by entering the following command:

```
gui_platform_cntrl start
```

Result: The command output depends on whether the system is a co-resident or a distributed configuration; refer to "gui_platform_cntrl command" (p. 11-10) for details regarding the command output.

END OF STEPS

Stop the GUI Web Server

When to use

Use this task to stop the GUI web server (GWS).

Related information

See the following topics in this document:

- "gui_platform_cntrl command" (p. 11-10)
- "View a List of User Accounts" (p. 8-14)
- "Processes" (p. 9-2)
- "Start the Platform" (p. 9-5)

Before you begin

Notify all users that the GUI web server is coming down and that they must be logged off of the management system.

Task

Complete the following steps to stop the GUI web server.

1 From the machine on which the management system is running, log in as **oms**.

Result: You are logged in as **oms**.

2 Stop the web server by entering the following command:

```
gui_platform_cntrl stop
```

Result: The web server is stopped.

3 Enter the following command to determine if the web server processes have been stopped:

```
gui_platform_cntrl status
```

Result: The command output should not display any running processes.

END OF STEPS

Start the NAs

When to use

Use this task to start the network adapter (NAs).

Related information

See the following topics in this document:

- "The operating processes platform commands" (p. 9-2)
- "Processes" (p. 9-2)
- "NAs" (p. 11-2)

Before you begin

The HP® servers, in which the management system software is loaded, must be up and running.

Read the "gui_platform_cntrl command" (p. 11-10) for details.

Task

Complete the following steps to start the network adapters (NAs).

1 From the machine on which the management system is running, log in as **cna**, **tna** or **nma**.

Result: You are now logged in as **cna**, **tna** or **nma**.

2 To determine if any application processes are running, enter the following command line:

```
platform_cntrl status
```

Result: The command output should not display any running processes.

3 Start the NA by entering the following command:

```
platform_cntrl start
```

Result: The command output depends on whether the system is a co-resident or a distributed configuration; refer to "gui_platform_cntrl command" (p. 11-10) for details regarding the command output.

END OF STEPS

Stop the NAs

When to use

Use this task to stop the network adapter (NAs).

Related information

See the following topics in this document:

- "The operating processes platform commands" (p. 9-2)
- "Processes" (p. 9-2)
- "NAs" (p. 11-2)

Before you begin

Notify all users that the NA is coming down and that they must be logged off of the management system.

Task

Complete the following steps to stop the NAs.

1 From the machine on which the management system is running, log in as **`cna`**, **`tna`** or **`nma`**.

Result: You are now logged in as **cna**, **tna** or **nma**.

2 Stop the NA by entering the following command:

```
platform_cntrl stop
```

Result: The NAs are stopped.

3 Enter the following command to determine if the NA processes have been stopped:

```
platform_cntrl status
```

Result: The command output should not display any running processes.

END OF STEPS

Restart the HP® Servers

When to use

Use this task to restart the HP® servers periodically. For HP® Serviceguard configurations, use this task on the standby nodes only.

Important! As routine system maintenance, perform this task every two months to improve server performance; see "Periodic Maintenance" (p. 41-2).

Related information

See the following topic in this document:

- "Periodic Maintenance" (p. 41-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to restart servers; and, for HP® Serviceguard configurations, complete the following steps on the standby nodes only.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to reboot the HP® servers gracefully:

```
shutdown -r
```

Result: The system gracefully shuts down all applications and restarts.

END OF STEPS

Change the Name of the Host HP® Server

When to use

Use this task to change the name of the host HP® server.

Related information

See the following topic in this document:

- "hostchange command" (p. 9-2)

Before you begin

Step one of this procedure requires you to complete the steps in the "Stop the Platform" (p. 9-7) task.

Task

Use this task to change the name of the host HP® server.

1 Complete the steps in the "Stop the Platform" (p. 9-7) task.

2 From the machine on which the management system is running, log in as **root**.

3 Enter the following command line:

```
. /opt/lucent/platform/bin/setup osm
```

4 Enter the following command line to change the host name:

```
hostchange --hostname <newhostname>
```

Where: **<newhostname>** is the name of the new host.

Example:

```
hostchange --hostname Rex
```

Result: The system searches for installed components and loads the necessary tasks. Output similar to the following is displayed.

```
Loading Component Info for ETCHOST...Done
...
Loading Component Info for ITorbixASP...Done
```

```
***Checking if any OMS/NA process(es) are running ***[*]
Done

/opt/lucent/platform/bin/hostchange will implement the
following changes:

New Hostname: Rex

New IP Address: No Changes
```

5 Enter **y** when the system prompts you to continue:

```
y
```

6 Reboot the HP® server by entering the following command:

```
reboot
```

Result: The HP® server comes up with the new host name. If Iona is installed and configured, an auto-restart script is deposited into **/sbin/rc3.d** that causes **hostchange** to restart itself and finish the regeneration of the Iona configuration.

END OF STEPS

Change the IP Address of the Host HP® Server

When to use

Use this task to change the IP address of the host HP® server.

Related information

See the following topic in this document:

- "hostchange command" (p. 9-2)

Before you begin

Step one of this procedure requires you to complete the steps in the "Stop the Platform" (p. 9-7) task.

Task

Use this task to change the IP address of the host HP® server.

1 Complete the steps in the "Stop the Platform" (p. 9-7) task.

2 From the machine on which the management system is running, log in as **root**.

3 Enter the following command line:

```
. /opt/lucent/platform/bin/setup osm
```

4 Enter the following command line to change the IP address of the host HP® server:

```
hostchange --ip <newIPaddress>
```

Where: **<newIPaddress>** is the new IP address.

Example:

```
hostchange --ip 135.99.99.99
```

Result: The system searches for installed components and loads the necessary tasks. Output similar to the following is displayed.

```
Loading Component Info for ETCHOST...Done
...
Loading Component Info for ITorbixASP...Done
```

```
***Checking if any OMS/NA process(es) are running ***[*]
Done

/opt/lucent/platform/bin/hostchange will implement the
following changes:

New Hostname: Np Changes

New IP Address: 135.99.99.99
```

5 Enter **y** when the system prompts you to continue:

```
y
```

6 Reboot the HP® server by entering the following command:

```
reboot
```

Result: The HP® server comes up with the new IP address. If Iona is installed and configured, an auto-restart script is deposited into **/sbin/rc3.d** that causes **hostchange** to restart itself and finish the regeneration of the Iona configuration.

END OF STEPS

Changing Host IP Address for MST zone

When to use

Use this procedure when you want to change the Host IP address for MST zone.

Related Information

See "Changing the IP Address for Southbound (EIU) Connection in MST Zone" (p. 9-20)

Before you begin

This task applies to Solaris platform only.

Task

Complete the following steps to change the Host IP Address for the MST Zone.

1 From MST zone, login as **oms**.

Bring down the application.

2 From global area, make the following changes:

- Login as **root**
- Enter the following command to find the name for MST zone:
  zoneadm list -p
- Enter the following command to halt MST zone:
  zoneadm -z *name_of_mst_zone* **halt**
- Enter the following commands to modify ZONE definition:
  zonecfg -z *name_of_mst_zone*
  zonecfg>remove net address=*old_ip*
  zonecfg>commit
  zonecfg>add net
  zonecfg>set address=*new_ip*
  zonecfg>end
  zonecfg>commit
  zonecfg>exit
- Enter the following command to modify IP info in zone key area:
  ZONE_DIR=$ (zoneadm -z *name_of_mst_zone* list -p | cut -d':' -f4)

Edit the following files and modify the IP stored:

1. **`$ZONE_DIR/root/etc/hosts`**
2. **`$ZONE_DIR/root/etc/inet/ipnodes`**

- Enter the following command to boot MST zone:
  `zoneadm -z` *name_of_mst_zone* **`boot`**

3 From the MST zone, make the following changes:

- Login MST zone as **root**
- Modify IP info stored in:
  `/var/opt/lucent/global/lan_mac_map`
- To modify the rest of the application area, refer to the "Change the IP Address of the Host HP® Server" (p. 9-16).

END OF STEPS

Changing the IP Address for Southbound (EIU) Connection in MST Zone

When to use

Use this procedure when you want to change the IP Address for Southbound (EIU) Connection in MST zone

Related Information

See "Changing Host IP Address for MST zone" (p. 9-18)

Before you begin

This task applies to Solaris platform only.

Task

Complete the following steps to change the IP Address for Southbound (EIU) Connection in MST zone.

1 From mst zone, login as **oms**.

2 Bring down the application.

3 From global zone, login as **root**.

4 Change the below directory:

```
cd /opt/lucent/container/bin
```

5 Run the following command to remove the old EIU LAN info:

```
./lt_oms_lan_config -d -z name_of_mst_zone -if ethernet_interface_name -ip old_ip_address
```

6 Run the following command to add the new EIU LAN info:

```
./lt_oms_lan_config -z name_of_mst_zone -if eithernet_interface_name -ip new_ip_address -subnet new_subnet_address -netmask new_netmask
```

Note: /var/opt/lucent/global/lan_mac_map will be re-generated with the new IP info.

7 From MST zone, login as **root**.

8 Run the following command to reconfigure the LAN interface used for SB connection:

```
/opt/lucent/platform/bin/lt_config
```

Note: /etc/opt/lucent/platform/tna_* will be recreated with new MAC address.

9 Login as **oms**.

10 Bring up the application.

END OF STEPS

Decompress a Compressed .gz File

When to use

Use this procedure to decompress a compressed **.gz** file.

Related information

This task does not have any related information.

Before you begin

This task offers you two ways to decompress a file: to decompress the file and to write it to standard output, which is shown in Step 3, or to decompress a file and to redirect the output to another file, which is shown in Step 4.

Task

Use this task to decompress a compressed **.gz** file.

1 From the machine on which the management system is running, log in as **oms**.

2 To decompress a file and to write it to standard output, go to Step 3.

To decompress a file and to redirect the output to another file, go to Step 4.

3 Enter the following command to decompress a file to standard output:

```
/usr/contrib/bin/gunzip -c <file to be compressed.gz>
```

Result: The file that you specified as **<file to be compressed.gz>** is decompressed to standard output. You have completed this task.

4 Enter the following command to decompress a file and to redirect the output to another file:

```
/usr/contrib/bin/gunzip -c <file to be compressed.gz> > <output
directory/output file>
```

Example:

```
/usr/contrib/bin/gunzip -c /tmp/alarm.log.gz > tmp/alarm.log
```

Result: The file that you specified is decompressed and its output is redirected to the file specified.

END OF STEPS

Eject a CD-ROM

When to use

Use this task to eject a CD-ROM when the CD-ROM does not get ejected as expected.

Related information

This task does not have any related information.

Before you begin

This task does not have any preconditions.

Task

Use this task to eject a CD-ROM when the CD-ROM does not get ejected as expected.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to change directories to the highest level:

```
cd /
```

Result: The directory is changed to the highest level directory.

3 Enter the following command lines to facilitate the ejection of the CD-ROM:

```
fuser -cku /SD_CDROM
umount /SD_CDROM
```

4 Press the **Eject** button to retrieve the CD-ROM from the drive.

Result: The CD-ROM is ejected.

END OF STEPS

Install Image Files as a Background Map

When to use

Use this task to install image files as a background map on all servers that have the management system GUI installed; meaning, the OMS server, the primary and/or secondary OMS servers for Disaster Recovery configurations, and all distributed GWSs.

Related information

This task does not have any related information.

Before you begin

This task is presented in two parts. Use part 1, which is done at the HP server, to run the script that installs the image files as the background map. Use part 2, which is done while logged on to the management system GUI, to select the image of the newly installed background map and to verify that the newly installed user selected background map is properly displayed.

Part 1 of this task requires you to have the appropriate image files in .gif, .jpg, or .shp format.

Task, Part 1: At the HP Server

Use this task to install image files as a background map.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Using ftp or rcp, copy the new image files to any directory on the OMS host:

```
cp <image filename> <directory>
```

3 Enter the following command to change directories:

```
cd /opt/lucent/platform/bin
```

4 Enter the following command to run the add_background_map script:

```
./add_background_map
```

5 When prompted, input the directory in which the image file resides and the filename of the image file.

6 To re-start the web server, enter the following command:

```
gui_platform_cntrl restart
```

Result: The system immediately returns the message: `Platform start requested`. Starting the web server takes up to 15 minutes to complete.

END OF STEPS

Task, Part 2: On the management system GUI

Use this task to select the image as user background map.

1 Log in to the management system.

2 Open the user preference page.

3 Select the newly added background from Map background list in the Map preference panel.

4 Click **Submit**.

5 Open a new Network Map page to verify that the new user selected background map is displayed.

END OF STEPS

Configure a Secure Shell (SSH)

When to use

Use this task to configure a secure shell (ssh), which sets up the .shost-based authentication between systems.

Related information

This task does not have any related information.

Before you begin

You might be asked to verify the authenticity of a server or you might be challenged for passwords.

Task

Use this task to configure a secure shell (ssh), which sets up the .shost-based authentication between systems.

1 On the primary server, enter the following command line:

```
sh /opt/lucent/toolbox/bin/lt_ssh_config_setup
```

2 On the secondary server, enter the following command line:

```
sh /opt/lucent/toolbox/bin/lt_ssh_config_setup
```

3 On the primary server, enter the following command line:

```
sh /opt/lucent/toolbox/bin/lt_ssh_allow_remote_server <secondary
server name>
```

Result: You may be asked to verify the authenticity of a server and may be challenged for a password. If so, provide appropriate responses. You should eventually be presented with a response from the secondary server.

4 To continue to set up .shost-based authentication between systems, enter the following command line on the secondary server:

```
sh /opt/lucent/toolbox/bin/lt_ssh_allow_remote_server <primary
server name>
```

Result: Once again, you may be asked to verify the authenticity of a server and may be challenged for a password. If so, provide appropriate responses. You should eventually be presented with a response from the primary server.

END OF STEPS

10 Backup, Recovery, and Restoration

Overview

Purpose

This chapter contains conceptual information and related tasks for the backup, recovery, and restoration operations that involve the management system.

Contents

System Backups

The operating principles of system backups

System backups are performed on the local HP® server in the **/backups** directory.

Once the backup is performed, the data that has been backed up can be stored by one or both of the following methods:

- Writing it to tape for the Server Platform
  Note that any data that is stored on tape can be read from tape to the **/backups** directory. See the "Write a System Backup to Tape " (p. 10-12) and "Read a System Backup from Tape" (p. 10-14) tasks for details.
- Writing it to another device and/or to the system for the Server Platform and/or the PC Platform

System backups adhere to the following operating principles:

- System backups are not file-selective; meaning, if the **/backups** directory houses other files (such as patches), these files are also backed up.
- If the backup is not stored on tape or on another device/system, the scheduled backup overwrites the previous backup. (See "View a List of Scheduled Hot System Backups" (p. 10-6) and "Modify a Scheduled Hot System Backup" (p. 10-7).)
- If a backup from tape is performed to the **/backups** directory, the backup that currently resides in **/backups** is overwritten.

Supported platforms for backups

Backups are supported on the Server Platforms and the PC Platform.

Important! Since the PC Platform does not support a tape drive, any write-to-tape or read-from-tape operations are not applicable; meaning, the"Write a System Backup to Tape " (p. 10-12) and "Read a System Backup from Tape" (p. 10-14) tasks are not applicable to the PC Platform.

Types of system backups

The management system offers system administrators the convenience of performing one of two types of backups:

- *Hot backups*, which are performed through the management system while the management system and the HP® servers are up and running; see the "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) task for details.
- *Cold backups*, which are performed through the command line interface on the HP® server while the management system is brought down; see the "Execute a Cold System Backup from the HP® Server" (p. 10-9) task for details.

Both the hot and cold backups back up the following to a local disk:

- OMS database
- Lightweight Directory Access Protocol (LDAP) database
- flat files, which do not include NE backups of flat files

The log files for both hot and cold backups can be found using the following path:

/var/opt/lucent/logs/db/archive.log

For the maintenance schedule involving system backups, see "Run hot system backups" (p. 41-1) and "Run cold system backups" (p. 41-2).

Hot system backups

The functions for a hot backup are supported from the **Administration > System Backups** page of the management system.

The System Backups page displays information that can be viewed or modified regarding the following:

- Schedule mode, which specifies whether backups are to be performed daily, weekly, once, or not at all (none)
- Date of the next backup
- Date of the last backup
- Status of the last backup
- System device, which is the **/backups** directory
- Device type
- In Progress

See the "View a List of Scheduled Hot System Backups" (p. 10-6), "Modify a Scheduled Hot System Backup" (p. 10-7), and "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) tasks for details.

For the maintenance schedule involving hot system backups, see "Run hot system backups" (p. 41-1).

Cold system backups

Because cold system backups are performed through the command line interface on the HP® server while the management system is brought down, the management system cannot be used to view a list of scheduled backups or to schedule or modify the schedule of any cold system backup. See the "Execute a Cold System Backup from the HP® Server" (p. 10-9) task for details.

For the maintenance schedule involving cold system backups, see "Run cold system backups" (p. 41-2).

System recoveries

System recoveries are performed using the output of hot or cold backups. (See the "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) or "Execute a Cold System Backup from the HP® Server" (p. 10-9) tasks for details.)

The recovery and restoration affects the OMS and Lightweight Directory Access Protocol (LDAP) databases of the management system and any required flat and configuration files. Restorations are performed using the backup images of each database. See the "Recover and Restore the Database" (p. 10-16) task for details.

Important! Backups and restorations only pertain to the OMS database. Backups of the NAs are not supported.

The following configurations are not supported:

- A backup from a coresident configuration and a restoration to a distributed configuration is not supported.
- A backup from a distributed configuration and a restoration to a coresident configuration is not supported.
- A backup from one distributed configuration and restoration to another distributed configuration with different set of servers is not supported.

Best time of the day for system and NE backups

System backups should be run when scheduled activities (cron jobs) are not running.

Between 22:00 P.M. and 03:00 A.M. various internal activities such as database purging and PM data collection occur; therefore, we recommend that you do NOT run system backups between this time period because they could overload the database. We recommend that you run system backups after 03:00 A.M.

In addition, we recommend that you run NE backups before 22:00 P.M.

Most scheduled activities can be changed via system parameters or the cron job if this recommended schedule is not acceptable or convenient for your installation, but such changes should only be done by those system administrators who understand the implications of making such changes.

To avoid scheduling operations simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

High Availability configurations and scheduled system backups

In a High Availability configuration, data inconsistencies can arise on the primary active and the secondary active management systems regarding scheduled backups. Backups have to be scheduled manually on the secondary active management system in order to have the data on that management system synchronized with the data that appears on the primary active management system. For additional details regarding High Availability configurations, refer to Chapter 21, "High Availability".

Frequency of system backups

For the maintenance schedule involving system backups, see "Run hot system backups" (p. 41-1) and "Run cold system backups" (p. 41-2).

Backup related platform alarms

The following hot links provide additional information on platform alarms that could be related to the malfunctioning of a backup:

- "BACKUP_DATABASE_NOW" (p. 42-8)
- "BACKUP_ERROR" (p. 42-9)

View a List of Scheduled Hot System Backups

When to use

Use this task to view a list of scheduled hot system backups.

Related information

See the following topic in this document:

- "System Backups" (p. 10-2)

Before you begin

The system can only have one system backup schedule. In addition, because of the innate nature of screen refreshing, the status of the Inprogress (Y/N) field might not be up-to-date.

Task

Complete the following step to view a list of scheduled hot system backups.

1 From the Administration home page, click on **System Backups**.

Result: The System Backups page is displayed, which lists the scheduled system backups.

END OF STEPS

Modify a Scheduled Hot System Backup

When to use

Use this task to modify a scheduled hot system backup.

Related information

See the following topic in this document:

- "System Backups" (p. 10-2)

Before you begin

The system can only have one system backup schedule.

Task

Complete the following steps to modify a scheduled system backup.

1 From the Administration home page, click on **System Backups**.

Result: The System Backups page is displayed, which lists the scheduled system backups.

2 In the Schedule Mode column, click on the hyperlink for the schedule to be modified.

Result: The View or Modify System Backup page is displayed.

3 Modify the appropriate information and press **Submit**.

Result: The system backup schedule is modified. The message `Operation completed successfully` is displayed.

END OF STEPS

Execute an Immediate Hot System Backup from the OMS

When to use

Use this task to execute an immediate hot system backup from the management system.

Related information

See the following topic in this document:

- "System Backups" (p. 10-2)

Before you begin

Verify that a system backup in not already in progress.

Task

Complete the following steps to execute an immediate system backup from the OMS.

1 From the Administration home page, click on **System Backups**.

Result: The backup process is automatically selected because only one backup can be scheduled at a time.

2 At the bottom of the page, click on **Backup now**.

Result: A pop-up window is displayed that asks:

```
Do you wish to continue with the backup? Please Confirm. Yes
or No?
```

3 If you click **Yes** to confirm the backup, the immediate backup is begun.

If you click **No** so the backup is not executed, the immediate backup is cancelled.

Result: If the message `Operation successfully completed` is displayed, the backup has begun.

The system indicates the status of the backup with the message: `Backup failed/succeeded`.

If the message `Backup failed, check /var/opt/lucent/logs/db/archive.log for details` is displayed, contact Alcatel-Lucent Customer Support Services to continue. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

END OF STEPS

Execute a Cold System Backup from the HP® Server

When to use

Use this task to execute a cold system backup of the OMS database, the Lightweight Directory Access Protocol (LDAP) database, and any required flat files, which do not include NE backups of flat files.

Related information

See the following topics in this document:

- "Recover and Restore the Database" (p. 10-16)
- "System Backups" (p. 10-2)

Before you begin

Verify that the Operations, Administration, and Maintenance (OAM) and OMS platform applications are shut down.

Task

Complete the following steps to execute a cold backup of the OMS database, the Lightweight Directory Access Protocol (LDAP) database, and any required flat or configuration files from the HP® server.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command:

```
su - oms
```

Result: The login is changed to **oms**.

3 Enter the following command to determine if the application is running:

```
platform_cntrl status
```

Result: The system outputs the status of the application, which is similar to the following:

```
Overall System status...[shutdown]

platform...[Down]

oms...[Down]

tna...[Down]
```

If the application is not running, go to Step 5.

If the application status is running, go to the next step.

4 Enter the following command to stop the application and the GUI web server:

```
platform_cntrl stop
```

Result: The application and the GUI web server are stopped.

5 Enter the following command to mount the database file systems:

```
platform_cntrl begin_maintenance
```

Result: Database file systems are mounted and the message `mounting is done successfully` is displayed.

6 Wait 30 seconds before executing the next command; or, verify that the file systems have been mounted by entering the following command:

```
mount | grep "osm/db/db06"
```

Result: If the **mount** command outputs a message, the file systems have been mounted. If the **mount** command does not output a message, the file systems have not been mounted.

7 Enter the following command to return to the root login:

```
exit
```

Result: The login is returned to **`root`**.

8 At the prompt, enter the following command to change directories:

```
cd /opt/lucent/platform/bin
```

Result: The directory is changed.

9 Enter the following command to set up the environment:

```
. ./setup osm
```

Result: The environment is set up.

10 Enter the following command to initiate the backup to the local disk:

```
db_backup
```

11 Wait for the backup to complete, and then read the messages to determine if the process has completed successfully.

Result: The backup is stored in the **/backups** directory.

If the message `Backup successfully completed` is displayed, go to Step 12.

If the message `Backup failed, check /var/opt/lucent/logs/db/archive.log for details` is displayed, contact Alcatel-Lucent Customer Support Services to continue. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

12 At the prompt, enter the following command:

```
su - oms
```

Result: The login is changed to **oms**.

13 Enter the following command to unmount the database file systems:

```
platform_cntrl end_maintenance
```

Result: Database file systems are unmounted and the message `umounting is done successfully` is displayed.

14 Enter the following command to start the application and the GUI web server:

```
platform_cntrl start
```

Result: The application and the GUI web server are started.

END OF STEPS

Write a System Backup to Tape

When to use

Use this procedure to write a system backup to tape for the HP® Server platform only.

Important! This procedure is not applicable to the OMS PC Platform.

Related information

See the following topic in this document:

- "System Backups" (p. 10-2)
- "Read a System Backup from Tape" (p. 10-14)

Before you begin

This procedure enables you to write management system database backup data to tape and NE backup data, which is in the form of flat files, to tape. If you choose to write both sets of backup data to tape, you will need two tapes.

Once you have completed this procedure, you can read the data from the tape using the "Read a System Backup from Tape" (p. 10-14) task.

Task

Complete the following steps to write a system backup to tape on the Server platform.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to initiate the writing of the backed up data to tape:

```
/opt/lucent/platform/bin/write_backup_to_tape
```

Result: The following prompt is displayed:

```
Please put in a blank tape and press [Enter] to continue.
```

3 Insert a blank tape and press **Enter**.

Result: The data is copied from the **/backups** directory to the tape.

4 Remove the tape, write protect the tape, and label the tape as follows:

Database Backup-mmddyyyy

Where: **mm** represents the current month of the year; **dd** represents the current day of the year; and **yyyy** represents the current year.

Result: The following prompt is displayed:

```
Do you want to save NE Backup to tape? (y|n)
```

5 If you want to continue to write NE backup flat files to tape, enter **y** at the prompt and go to Step 6.

If you do not want to continue to write NE backup flat files to tape, enter **n** to exit. You have completed this procedure.

Result: If you entered **y** to continue, the following prompt is displayed:

```
Please put in a new blank tape and press [Enter] to continue.
```

6 Insert another blank tape at prompt and press **Enter**.

Result: The data is copied from the **/var/opt/lucent/ftp/pub/obr** directory to the tape.

7 Remove the tape, write protect the tape, and label the tape as follows:

NE Backup-mmddyyyy

Where: **mm** represents the current month of the year; **dd** represents the current day of the year; and **yyyy** represents the current year.

END OF STEPS

Read a System Backup from Tape

When to use

Use this procedure to read a system backup from tape for the HP® Server Platform.

Important! This procedure is not applicable to the OMS PC Platform.

Related information

See the following topics in this document:

- "System Backups" (p. 10-2)
- "Recover and Restore the Database" (p. 10-16)

Before you begin

This procedure enables you to read management system database backup data from tape and NE backup data, which is in the form of flat files, from tape. If you choose to read both sets of backup data from tape, you will need to have the two tapes that store this data, which should be labeled **Database Backup-mmddyyyy** and **NE Backup-mmddyyyy**.

This procedure overwrites the data that is currently stored in the **/backups** directory.

Ensure that the tape is write-protected.

Task

Complete the following steps to read a system backup from tape for the HP® Server Platform.

1 From the machine on which the management system is running, log in as `root`.

2 Enter the following command line to initiate the database backup from the tape:

```
/opt/lucent/platform/bin/read_backup_from_tape
```

Result: When the following prompt appears, go to step Step 3:

```
Please insert the Database Backup tape and press [Enter] to
continue.
```

3 Insert the database backup tape and press **Enter**.

Result: If the following prompt is displayed, another backup exists on the server. Go to step Step 4 to overwrite the existing backup or go to Step 5 to exit.

If the following prompt does not appear, the data is read from the database backup tape and put into the **/backups** directory. Go to step Step 6.

```
Backup directory /backups already contains a backup!!!

Contents are:

DATE: 20041201.1351

HOST: tellus

HOSTIP: 135.112.92.35

LOGICALNAME: tellus

BACKUPMODE: HOT

Do you want to overwrite this backup, and continue? (y/n):
```

4 Enter **y** if existing the database backup can be overwritten (discarded), and continue to Step 6.

Result: The data is read from the tape and put into the **/backups** directory.

5 Enter **n** to exit the database backup and go to Step 6.

6 Remove the database backup tape.

Result: The following prompt appears:

```
Do you want to restore NE Backup data? (y|n)
```

7 Enter **y** to continue the restoration of the NE backup and go to Step 8.

Enter **n** to skip the restoration of the NE backup. You have now completed this procedure.

8 Insert the NE backup tape and press **Enter**.

Result: The data is read from the tape and put into the **/var/opt/lucent/ftp/pub/obr** directory.

9 Remove the NE backup tape.

END OF STEPS

Recover and Restore the Database

When to use

Use this task to restore the network databases from tape or the local disk. This task contains steps to recover and restore the OMS and Lightweight Directory Access Protocol (LDAP) databases and any required flat or configuration files. Restorations are performed using the backup images of each database.

Related information

See the following topics in this document:

- "Read a System Backup from Tape" (p. 10-14)
- "Execute a Cold System Backup from the HP® Server" (p. 10-9)
- "Execute an Immediate Hot System Backup from the OMS" (p. 10-8)
- "System recoveries" (p. 10-4)

Before you begin

The use of *disk* in this task refers to the hard drive.

Certain configurations are not supported for recoveries and restorations; refer to the "System recoveries" (p. 10-4) for details.

Task

Complete the following steps to recover and restore the database.

1 If the backup data is stored on tape, complete the steps listed in the "Read a System Backup from Tape" (p. 10-14) task and go to Step 3.

If the backup data is stored on the local disk, go to Step 2.

2 From the machine on which the management system is running, log in as **root**.

3 Enter the following command:

```
su - oms
```

Result: The login is changed to **oms**.

4 Enter the following command to determine if the application is running:

```
platform_cntrl status
```

Result: The system outputs the status of the application, which is similar to the following:

```
Overall System status...[shutdown]
platform...[Down]
oms...[Down]
tna...[Down]
```

If the application is not running, go to Step 6.

If the application status is `running`, go to the next step.

5 Enter the following command to stop the application and the GUI web server:

```
platform_cntrl stop
```

Result: The application and the GUI web server are stopped.

6 Enter the following command to mount the database file systems:

```
platform_cntrl begin_maintenance
```

Result: The database file systems are mounted.

7 Wait 30 seconds before executing the next command; or, verify that the file systems have been mounted by entering the following command:

```
mount | grep "osm/db/db06"
```

Result: If the **mount** command outputs a message, the file systems have been mounted. If the **mount** command does not output a message, the file systems have not been mounted.

8 Enter the following command to return to the root login:

```
exit
```

Result: The login returns to **`root`**.

9 Enter the following command to change directories:

```
cd /opt/lucent/platform/bin
```

Result: The directory is changed.

10 Enter the following command to set up the environment:

```
. ./setup osm
```

Result: The environment is set up.

11 Enter `db_restore` and press **Enter** to restore all areas of the database.

Result: The database restore begins.

12 Answer **yes** or **no** when the system prompts you:

```
Do you want to use NE(s) in the NA database? (y/n).
```

Enter **y** and press the **Enter** key to get a superset of the NE list from the OMS and NA databases.

Enter **n** and press the **Enter** key to get an NE list based upon the Navis OMS databases only.

Press the **Enter** key to take the default, which varies according to the system configuration.

Result: Depending on what you have selected, a message similar to the following is displayed:

```
NE List Sync will be <SUPERSET> based, press [ENTER] to
continue.
```

13 Press **Enter**.

14 Once the restoration is started, read the system messages to determine if the restoration process completed successfully.

Result: If the message `Restore successfully completed` is displayed at the end, the OMS database restoration completed successfully. Go to the next step.

If the following message is displayed at the end, the restoration did not successfully complete; contact Alcatel-Lucent Customer Support Services to continue. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

```
Restore failed, check /var/opt/lucent/logs/db/restore.log for
details.
```

15 At the prompt, enter the following command:

```
su - oms
```

Result: The login is changed to **oms**.

16 Enter the following command to unmount the database file systems:

```
platform_cntrl end_maintenance
```

Result: Database file systems are unmounted.

17 Enter the following command to start the application and the GUI web server:

```
platform_cntrl start
```

Result: The application and the GUI web server are started.

18 Initiate a database synchronization for each NE once the NE communication state is up and the `sync needed status` is `YES`.

If the `sync needed status` is `YES`, go to Step 19.

19 Log in to the management system.

20 Navigate to the Database Synchronizations page using the following path:

Tools > Database Synchronizations

Result: The Search for Database Synchronization page is displayed.

21 Select **All NEs in the network** and click the **Search** button.

Result: The Database Synchronizations page is displayed.

22 Look for any Database Synchronization Type that has a **Yes** in the Sync Needed column of the Database Synchronizations page.

END OF STEPS

Switch Over from an Active HP® Server to Cold Standby HP® Server

When to use

Use this task to switch over from a primary active HP® server to a secondary cold standby HP® server.

Related information

See the following topics in this document:

- "Processes" (p. 9-2)
- "System Backups" (p. 10-2)

Before you begin

Typically, a cold standby configuration consists of a primary active HP® server and a secondary HP® server that is kept pre-loaded with OMS software, but is not connected to the network. Copies of the OMS database and associated files are transferred from the primary to the cold standby server. The primary and the secondary cold standby servers can be co-located or they can be in geographically diverse sites. A permanent TCP/IP connection between the primary and the secondary servers is not required, which does attribute to a longer switchover time and a greater amount of data loss following a failover.

Before you begin to switch over from the active to the cold standby HP® server, realize that the success of the switchover relies on the quantity and the quality of the backups that were made from the data residing on the active server.

The switchover itself is a manual process that is identical to the procedure that would be used to restore the management system on a new server, which would be done if an event, such as a building fire, occurred. However, since the cold backup server is readily available, the downtime would be minimized.

The actual tasks that have to be completed on the cold standby and the time required to get the cold standby server on-line depend on how up-to-date the cold standby has been kept.

Task

Complete the following steps to switch over from the active to the cold standby HP® server.

1 If the application is not loaded on the cold standby, load the application and all appropriate software. (The software installation can take approximately 4 to 8 hours.)

2 If all software is installed on the cold standby, but the database is empty, restore the production database. (The restoration of the production database can take approximately 4 hours.)

Refer to the "Recover and Restore the Database" (p. 10-16) task for guidance.

3 If a restored production database resides on the cold standby, but the application is down, bring up the application. Note: If the latest production database was periodically restored on the cold standby, the cold standby would have to have been brought down. A database restoration is never performed on a running system. (Bringing up the application can take approximately 15 minutes.)

Refer to the "Start the Platform" (p. 9-5) task for guidance.

4 If all processes are running on the cold standby, but the cold standby is disconnected from the network, reconnect and resynchronize the cold standby with the network. (The reconnection and resynchronization with the network can take approximately 1 hour.)

END OF STEPS

11 Co-Resident and Distributed Architectures

Overview

Purpose

This chapter contains conceptual information and the tasks that are related to the co-resident and distributed architecture components of the management system.

Important! For the various distributed architecture configurations that include network adapter (NA) servers, Bulk Performance Monitoring (BPM) servers, and GUI web servers (GWSs), contact your Alcatel-Lucent local customer service support team.

Contents

NAs

NA definition

A network adapter (NA) is a component of the management system that accommodates the native command languages (CMISE and TL1) and transport structures (SONET and SDH) used by various types of network elements (NEs) so they are compatible with management system processing requirements.

Note: NMA is a new network adaptor (NA) introduced in R6.3. OMS only support co-resident NMA, no distributed NMA. NMA is a network adaptor to support 1671 Service Connect (SC) NEs.

NA functionality

Networks that include NAs can afford users with the following networking solutions and cost saving measures:

- For networks with widely distributed NEs, the NA can be near to the NEs that is supports, which reduces DCN problems.
- For large networks, multiple NAs can reduce the load on the main server by distributing the processing requirements for DCN communication and normalizing the NE models. Using low cost servers for the NAs is a cost effective way to scale system capacity because increasing the size of the main server is an expensive proposition due to third party software involved.

NA supported platforms

The use of a network adapter (NA) is supported on the *Server Platforms*.

An NA is not supported on the *PC Platform*.

NA as a licensable feature

The use of a network adapter (NA) is an optional licensed feature that is only available to customers who have purchased and installed this feature. See Chapter 5, “Licensing” and “OMS_NA license” (p. 5-9) for details.

NA types

The management system supports the following NA types:

- CMISE NAs, which are known as *CNA*s. The status of these NAs can be checked with the “Check CNA Status” (p. 11-19) task.
- TL1 NAs, which are known as *TNA*s. The status of these NAs can be checked with the “Check TNA Status” (p. 11-20) task.
- NMA NAs, the NMA network adapter is applicable only for 1671 Service Connect (SC) NEs. The status of these NAs can be checked with the “Check NMA Status” (p. 11-21) task.

Co-Resident and Distributed NA configurations

OMS supports co-resident and distributed network adapter configurations.

In a *co-resident* NA configuration, the management system and the supported NA reside on the same HP® server.

The following co-resident configurations are supported:

- One HP® server, in which OMS, TNA, CNA and NMA reside on that HP® server.
- One HP® server, in which OMS and TNA reside on that HP® server.
- One HP® server, in which OMS and CNA reside on that HP® server.
- One HP® server, in which OMS and NMA reside on that HP® server.

In a *distributed* NA configuration, the management system and the NAs are detached from the same HP® server and run on a separate, dedicated HP® servers. The supported hardware for the detached NA servers include the HP® rp3410 server.

The following distributed configurations are supported:

- Distributed CNA, in which OMS and TNA reside on the main HP® server; multiple CNAs each reside on separate HP® servers for NAs.
- Distributed CNA/TNA, in which OMS resides on one HP® server; multiple CNAs and TNAs each reside on separate HP® servers for NAs.

Note the following conditions:

- A configuration in which a NMA is distributed on a separate HP® Server from the main OMS HP® Server is not supported.
- A separate HP® server that is designated as an NA server can only host a single instance of an NA, which can be either a TNA or a CNA.
- A configuration in which a CNA is co-resident with OMS on the *main* HP® server and the TNA resides on a separate HP® server is not supported.

Reconfiguring with co-resident or distributed NA

For details regarding how to reconfigure with co-resident or distributed TNA/CNA configuration, refer to the following for more details: "TNA/CNA reconfiguration" (p. 11-13), "General reconfiguration assumptions" (p. 11-14), "Reconfigure OMS to Add Distributed TNA/CNA" (p. 11-26) , "Reconfigure OMS to Remove Distributed TNA/CNA" (p. 11-28), "Reconfigure OMS to Add Co-resident TNA/CNA" (p. 11-30) and "Reconfigure OMS to Remove Co-resident TNA/CNA" (p. 11-33) task.

NE backups for distributed configurations

The backup of NE flat files is not included as part of the OMS system backup. The backup of NE flat files is done on the NA server providing that the NA is not co-resident with the main server.

High Availability configurations and NAs

The distributed/multiple network adapter configurations support high availability options with duplicated main OMS hosts where the network connection data of the backup host is kept current with that of the active host. High availability with distributed NAs is supported through manual procedures to move NEs between NA. The NAs do not store any data that is not recoverable from the NEs and from the OMS application; therefore, the NAs do not require a database backup or restore.

NEs and NCGs

To move NEs easily among the NA servers, NEs can be organized into control groups and the control groups can be moved among the NAs, which streamlines the process in reaction to NA failures. These control groups are known as *Network Communications Groups* or *NCGs*. Whenever NEs are moved among NAs, the NAs to which NEs are added resynchronize with the network to regain management functions.

The NA and application start up

For a co-resident configuration, the NA starts up and shuts down with the management system.

For a distributed configuration, the following guidelines apply to the NA start up:

- The software on each server is started independently—the communication protocols already provide for the various cases of server start up orders.
- During the NA server start up, the "OMS_NA license" (p. 5-9) is checked. Start up is rejected if the license is not valid. The license includes the number of CPUs that are licensed, which is also checked. The NA server can contain a TNA, a CNA, or a NMA whichever NA is found is started.

The loss and restoration of the application

With distributed NAs, the management system can lose communications with an NA, which results in the generation of an alarm. While communications are down, any user actions that involve messages to the NA fail or become unavailable. When the connection is re-established, the management system performs an NE list and an alarm resynchronization with the NA.

NTP

The NA servers and main application server must be synchronized using Network Time Protocol (NTP); therefore, the NA server must be configured as NTP clients with the main application server or an external source as the NTP server. The main application server can be configured to be an NTP client for an external source or to free run.

NA related platform alarms

The following hot links provide additional information on platform alarms that are related to the malfunctioning of a NA configuration:

- "NA_ASSOC_LOST" (p. 42-20)
- "NA_COMMS_ERROR" (p. 42-20)

NAs and the Data Extraction Tool

The following hot link provides additional information to consider regarding NAs and the Data Extraction tool: "Data Extraction and Co-Resident and Distributed Architectures" (p. 16-4).

BPM

BPM definition

Bulk Performance Monitoring (BPM) is licensable feature that enables 15 minute and 24 hour performance monitoring data to be collected on all monitoring points in the network. A monitoring point consists of a termination point, a monitoring rate, and associated granularity.

As its name implies, Bulk Performance Monitoring is designed to collect a large volume of data; and as such, it places a larger load on the system, requires additional hardware, and places limitations on the DCN topology of the respective network.

BPM functionality

BPM interworks with a network adapter (NA) to collect data from NE; it functions as a proxy for the NA.

The NA spools data that is associated with a PM request and sends that data to BPM. BPM then generates files that contain the new data and bulk loads that data into the management system database. Cron-controlled scripts are then run to merge any updated information into the database.

Each NA is associated with one BPM instance. One BPM instance can be associated with one or more NAs.

Each management system can have one and only one BPM instance.

BPM supported platforms

The use of Bulk Performance Monitoring (BPM) is supported on the *Server Platforms*.

BPM is not supported on the *PC Platform*.

BPM as a licensable feature

The use of Bulk Performance Monitoring (BPM) is an optional licensed feature that is only available to customers who have purchased and installed this feature. See Chapter 5, “Licensing” , “OMS_BPM license” (p. 5-4), and “OMS_PM_SERVER license” (p. 5-12) for details.

BPM modes of collection

OMS provides users with the ability to collect Performance Monitoring (PM) data from the NEs and to store that data in the management system database.

OMS offers two modes in which PM data can be collected:

- In *Selected-port mode*, users can specify the network connections, the NEs, and the specific ports for which PM data is to be collected. The management system then collects PM data only for those specified points:
  24-hour PM data is collected once per day, and it can be stored for up to 62 days. 15-minute PM data is collected multiple times each day, and it can be stored up to 14 days. Note that when 15-minute PM data is collected in selected-port mode, it is subject to the limitations of the total number of ports for which PM data can be collected.
- In the *Bulk mode*, which is supported for directly managed TL1 and CMISE NEs, a greater volume of data collection and storage occurs because the management system collects data for all ports in the network for which PM is enabled.
  Note that the hardware platform and DCN topology must be taken into account when determining the quantity of PM data that can be collected and stored when using bulk mode. Maximum storage in bulk mode is 31 days for 24-hour data and 7 days for 15-minute data.
  A distributed, dedicated PM application server is required for bulk mode data collection.

Reconfiguring with co-resident or distributed BPM

For details regarding how to reconfigure with co-resident or distributed BPM configuration, refer to the following for more details: “BPM reconfiguration” (p. 11-13), “General reconfiguration assumptions” (p. 11-14), “Reconfigure OMS to Add Distributed BPM Module” (p. 11-35), “Reconfigure OMS to Remove Distributed BPM Module” (p. 11-40) and “Reconfigure OMS to Remove Co-resident BPM module” (p. 11-41) task.

BPM and application start up

For a co-resident configuration, the Bulk Performance Monitoring (BPM) module starts up and shuts down with the management system.

For a distributed configuration, the following guidelines apply to Bulk Performance Monitoring (BPM) and application start up:

- The software on each server is started independently—the communication protocols already provide for the various cases of server start up orders.
- During the BPM server start up, the “OMS_PM_SERVER license” (p. 5-12) is checked. Start up is rejected if the license is not valid. The license includes the number of CPUs that are licensed, which is also checked.

BPM status

The status of BPM can be checked with the “Check BPM Status” (p. 11-22) task.

The loss and restoration of the application

The management system can lose communications with BPM, which results in the generation of an alarm.

NTP

The BPM server and management system server must be synchronized using Network Time Protocol (NTP); therefore, the BPM server must be configured as an NTP client with the management system server or an external source as the NTP server. The management system server can be configured to be an NTP client for an external source or to free run.

Scheduled activities management

BPM is triggered to start collecting 15 minute data every 15 minutes by an internal timer, which is known as a *cron job*.

The cron jobs are run from the server time zone, which is the UNIX® clock. The cron jobs run during a quiet period, which occurs from midnight on the UNIX® clock. For time details and the names of the BPM cron jobs, refer to the “Table of scheduled activities” (p. 41-4).

BPM related platform alarms

The following hot links provide additional information on platform alarms that are related to the malfunctioning of a BPM configuration:

- “BPM_15M_DATA_PURGED” (p. 42-9)
- “BPM_24H_DATA_PURGED” (p. 42-9)

BPM and the Data Extraction Tool

The following hot link provides additional information to consider regarding BPM and the Data Extraction tool: “Data Extraction and Co-Resident and Distributed Architectures” (p. 16-4).

GWSs

GWS definition

The GUI web server (GWS) is the component of the management system that provides OMS (management system) GUI functionality.

The GUI web server consists of the following processes:

- the Apache http process
- the tomcat process

GWS supported platforms

The use of a GUI web server (GWS) is supported on the *Server Platforms*.

The GWS is not supported on the *PC Platform*.

GWS as a licensable feature

The use of a GUI web server (GWS) is an optional licensed feature that is only available to customers who have purchased and installed this feature. See Chapter 5, “Licensing” and “OMS_GWS license” (p. 5-8) for details.

GWS configurations

OMS supports the following methods of GUI web server (GWS) configurations:

- In a *co-resident GWS configuration*, the management system and the supported GWS reside on the same HP® server.
- In a *distributed GWS configuration*, the management system and the supported GWS reside on the separate HP® servers. One or more GWSs are supported, thereby allowing more users to be logged in simultaneously.
  In addition, in a distributed GWS configuration, the management system GUI can only be accessed using the URL of a distributed GWS. An attempt to access the management system GUI using the URL of the OMS server returns a `Page not found` error.

Reconfiguring with co-resident or distributed GWS

For details regarding how to reconfigure with co-resident or distributed GUI web server configuration, refer to the following for more details: “GWS reconfiguration” (p. 11-14), “General reconfiguration assumptions” (p. 11-14), “Reconfigure OMS to Add Distributed GUI Web Server” (p. 11-42) , “Reconfigure OMS to Remove Distributed GUI Web Server” (p. 11-44), “Reconfigure OMS to Add Co-resident GUI Web Server” (p. 11-46) and “Reconfigure OMS to Disable Co-resident GUI Web Server” (p. 11-49) task.

gui_platform_cntrl command

The **gui_platform_cntrl** command is used to start and stop the GUI web servers (GWSs) and to view its status. From the OMS server, the command is executed with the appropriate option:

Command Format:

gui_platform_cntrl <start/stop/status>

Where:

start is used to bring up the GWSs.

stop is used to bring down the GWSs.

status is used to view the status of the GWSs.

As with the OMS server, users can log in to a distributed GUI web server as **oms** and use the **gui_platform_cntrl** command, which is available for each distributed GUI web server.

With this command, users can control the operation of the GUI web server on the *box* into which they are logged in. So, individual control of each distributed GUI web server can be accomplished by logging into the distributed GUI web server computer as **oms** and executing the **gui_platform_cntrl** command.

When the GUI web server resides in a distributed configuration, it is started and stopped as the GUI web server would be in the co-resident configuration. Refer to the "Start the Platform" (p. 9-5) , the "Start the GUI Web Server" (p. 9-9), the "Stop the GUI Web Server" (p. 9-10) tasks for details.

Unlike the co-resident configuration, the command output from a distributed configuration for a **gui_platform_cntrl start** or **gui_platform_cntrl stop** indicates that the command was sent to the distributed GUI web servers. In a co-resident configuration, feedback is output when the operation is complete. In a distributed configuration, the user must execute a **gui_platform_cntrl status** command to determine when the start/stop operation has been completed.

apache_config command

The **apache_config** command, which is executed as **root** from the command line of the machine on which the management system is loaded, is used to control hypertext transport protocol (HTTP) access to the OMS GUI web server by defining the set of TCP/IP addresses that are allowed to be serviced by OMS http process. By default, all TCP/IP addresses are allowed HTTP access to the OMS web server, but this set of addresses can be restricted using this command.

Command Format:

apache_config [-a <TCP/IP identifier> [-v] [-h]

Where:

-a is used to allow a domain.

<TPC/IP identifier> is in the format of:

{<*all*> <full/partial IP address> <network/netmask pair>}

-v is used to view all of the domains allowed.

-h is used to request command help.

Examples:

apache_config -a all allows all domains.

apache_config -a 999.99.99.99 allows the full IP address of 999.99.99.99.

apache_config -a 999.99 allows the partial IP address of 999.99.

apache_config -a 10.1.0.0/255.255.0.0 allows the network/netmask pair.

Refer to the "Allow a Domain for the GUI Web Server" (p. 11-24) and "View the Domain Allowed for the GUI Web Server" (p. 11-25) tasks for instructions.

Terminal Servers

Terminal server definition

Terminal servers are computers that allow the display of running server applications to be exported to a user's local workstation. Therefore, the burden of running the associated applications is delegated to the terminal server computer and the user's local workstation is only responsible for the graphical display of the terminal server application.

Terminal server supported platforms

Terminal servers are supported on the *Server Platforms* and the *PC Platform*.

Terminal servers types

Two types of terminal server computers can be deployed for a OMS application:

- A *Windows® Terminal Server*, which is a Windows-based server that can export an IE® browser session from the terminal server computer to the user's local workstation. The user can access the management system GUI by invoking an IE® browser on the terminal server and having the browser session display on the user's local workstation.
- An *ITM-SC Terminal Server*, which is designed for optical management system products that are configured with an ITM-SC element management system (EMS). The ITM-SC Terminal Server can be deployed so the ITM-SC GUI runs on one or more UNIX® computers and exports the associated ITM-SC GUI X-Window display to the user's local workstation.
  Important! The information in this document is dedicated to the description of the Windows® terminal services feature, which the OMS management system supports. Refer to the ITM-SC documentation for more information on ITM-SC terminal services.

Terminal server specifications

The terminal server meets a minimum specification with regard to number of CPUs, CPU speed, memory, and disk space; and it runs one of the supported Windows operating systems. The number of user sessions that it supports depends upon the server specification. The display is exported to users' desktops using Citrix® software, which accommodates UNIX®, X-terminal, and Windows® environments.

Number of CPUs	CPU Speed	Memory	Disks
4	2 GHz	8 GB	1 x 73 GB
2	2 GHz	4 GB	1 x 73 GB
4	1500 MHz	4 GB	3 x 36 GB
4	700 MHz	4 GB	3 x 9 GB

Terminal server and Exceed setup

Terminal Server and Exceed setup information is provided by the following OMS web page:

http://<hostname>/osm/jsp/ea/core/CutThroughSetup.jsp

Reconfigure OMS between Co-resident and Distributed Configuration

System components supported for reconfiguration

To benefit from the expansion of the OMS network, the management system supports the reconfiguration from a co-resident configuration, which is a *single box* configuration, to a distributed configuration for the following system components:

- TL1 Network Adapters (TNAs) or CMISE Network Adapters (CNAs); see "TNA/CNA reconfiguration" (p. 11-13) for details.
- Bulk Performance Monitoring (BPM); see "BPM reconfiguration" (p. 11-13) for details.
- GUI web servers (GWSs); see "GWS reconfiguration" (p. 11-14) for details.

The reconfiguration of these components from a co-resident configuration to a distributed configuration involves the following general steps:

- The distributed application server is installed.
- The corresponding component (TNA, CNA, BPM, GWS) is disabled on the co-resident configuration.
- If needed, any applicable licenses are installed.
- Optionally, any data associated with the application from the co-resident server can be migrated to the distributed server.
- The management system application is brought up on the distributed server.

TNA/CNA reconfiguration

The reconfiguration of TL1 Network Adapters (TNAs) or CMISE Network Adapters (CNAs) to be distributed enables the data that associates NEs and NAs to be reorganized in the management system database. This reconfiguration accommodates additional network growth and improves existing management system capacity.

BPM reconfiguration

The reconfiguration of Bulk Performance Monitoring (BPM) to be distributed enables PM processing to be relocated from the main HP® server in which the management system is running to a distributed HP® server configuration. This reconfiguraiton can improve the performance of the management system and increase the capacity of PM data collection and setting.

BPM is used to store and process PM data for TL1 Network Adapters (TNAs) or CMISE Network Adapters (CNAs) or NMA Network Adapters (NMAs). Regardless of the number of co-resident and distributed TNAs, CNAs and NMAs that the management system manages, the BPM reconfiguration to distributed configuration only includes one BPM server for both TNA, CNA and NMA.

Once OMS configured with distributed BPM, it cannot be reconfigured with co-resident BPM.

If BPM is running in a co-resident configuration, the "OMS_BPM license" (p. 5-4) needs to be purchased and installed during the reconfiguration to a distributed configuration.

GWS reconfiguration

The reconfiguration of a GUI web server (GWS) to be distributed enables the GWS to be relocated from the main HP® server in which the management system is running to a distributed HP® server configuration. This reconfiguration enables the number of management system users to be increased.

General reconfiguration assumptions

The following general assumptions apply the reconfiguration of all supported system components (TNA/CNA, BPM, and GWS):

- Reconfiguration is only supported within the same release of the management system. If a reconfiguration is needed from a previous management system release in which the application is running in a co-resident configuration, users must first upgrade to the current release of the management system and then proceed with the reconfiguration to a distributed configuration.
- During the reconfiguration procedure, it might be necessary to bring down the management system application in order to build the association between applications. This downtime would be minimal.

For specific areas of consideration, refer to the particular system component.

The lt_remove_bundle command

The **lt_remove_bundle** is used in the reconfiguration procedure, specifically during the "Reconfigure OMS to Remove Co-resident TNA/CNA" (p. 11-33) and "Reconfigure OMS to Remove Co-resident BPM module" (p. 11-41) tasks.

After the user executes the **lt_remove_bundle** command, the following dialog occurs. Commented lines with suggested user input are prefaced with asterisks.

Example:

***Enter 2 to choose the feature/bundle that you want to remove.

The dialog begins by resembling the following:

```
Preparing CONSOLE Mode Installation...

================================================

OMS  (created with InstallAnywhere by Macrovision)

------------------------------------------------

================================================

Uninstall OMS

-------------

About to uninstall...

OMS

This will remove features installed by InstallAnywhere.  It will not
  remove

files and folders created after the installation.




PRESS ENTER TO CONTINUE:



***Press the Enter key to continue with the uninstall.

===============================================
```

The dialog continues with un-install options:

```
Uninstall Options

-----------------



ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS ENTER TO ACCEPT THE
  DEFAULT:
```

```
  ->1- Completely remove all features and components.

    2- Choose specific features that were installed by
   InstallAnywhere.



Please choose one of the following options:





***Enter 2 to choose the feature/bundle that you want to remove.
```

The dialog then requests you to select product features:

```
===============================================

Choose Product Features

-----------------------



ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES
   YOU WOULD

LIKE TO SELECT, OR DESELECT.  TO VIEW A FEATURE DESCRIPTION, ENTER
   '?NUMBER'.  PRESS RETURN WHEN YOU ARE DONE.



1- [ ] OMS

    2- [ ] CNA

  3- [ ] NMA

    4- [ ] TNA

    5- [ ] BPM

    6- [ ] GWS
```

```
Check the features that you want to uninstall. Unchecked features
  will

   remain installed:




***Enter the number corresponding to the feature/bundle that you

   want to remove.
```

The output then performs the un-install:

```
===============================================

Uninstalling...

---------------

*************************



Cleaning up <bundle> associated File Systems...

Cleaning up cron files...

Cleaning up password and home directory ...

Removed bundle(s): bundles removed on Tues Nov 7 15:15:46 est
  2006...

===============================================

Uninstall Complete

------------------



All items were successfully uninstalled.
```

Recover from a Failed NA

When to use

Use this procedure to recover from a failed network adapter (NA).

Related information

See the following topic in this document:

- "NAs" (p. 11-2)

Before you begin

Before you begin to recover failed NAs, sufficient spare capacity should remain on the NA servers so if one NA server fails, the other NA servers can take up the load. Two methods to use would be the following:

- Set up 1+1 pairs in which one server remains unused as standby for each used NA.
- Set up an N:1 scheme.
  For example, have five NA servers each at 80% capacity. If one NA server fails, a quarter of the NEs could be transferred to each of the remaining NA servers.

In addition, network communication groups (NCGs) would have to be created so the NEs within the NCGs could be managed from an alternative NA server. The design of the data communication network must be considered for this step to be done.

Task

Complete the following step to recover from a failed network adapter (NA) state:

1 Using the steps provided in the *OMS Network Element Management Guide*, go to the Modify Network Communications Group (NCG) task and for each network communications group that is affected, change the NA server name to the planned alternative NA server name.

Result: The management system automatically transfers the NEs in the modified NCG to an alternate NA server and reconnects to each of the transferred NEs.

2 Using the steps provided in the *OMS Network Element Management Guide*, perform a database synchronization.

END OF STEPS

Check CNA Status

When to use

Use this task to check the status of a CMISE network adapter (CNA).

Related information

See the following topic in this document:

- "NAs" (p. 11-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check the status of a CMISE network adapter (CNA):

1 From the machine on which the CNA is installed, log in as **oms**.

2 Enter the following command line to check CNA status:

```
platform_cntrl status cna
```

Result: The system outputs CNA status.

END OF STEPS

Check TNA Status

When to use

Use this task to check the status of a TL1 network adapter (TNA).

Related information

See the following topic in this document:

- "NAs" (p. 11-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check the status of a TL1 network adapter (TNA).

1 From the machine on which the TNA is installed, log in as **oms**.

2 Enter the following command line to check TNA status:

```
platform_cntrl status tna
```

Result: The system outputs TNA status.

END OF STEPS

Check NMA Status

When to use

Use this task to check the status of a NMA network adapter (NMA).

Related information

See the following topic in this document:

- "NAs" (p. 11-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check the status of a NMA network adapter (NMA).

1 From the machine on which the NMA is installed, log in as **`oms`**.

2 Enter the following command line to check NMA status:

```
platform_cntrl status nma
```

Result: The system outputs NMA status.

END OF STEPS

Check BPM Status

When to use

Use this task to check Bulk Performance Monitoring (BPM) status.

Related information

See the following topic in this document:

- "BPM" (p. 11-6)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check BPM status.

1 From the machine on which the BPM is installed, log in as **oms**.

2 Enter the following command line to check BPM status:

```
platform_cntrl status bpm
```

Result: The system outputs BPM status.

END OF STEPS

Check GWS Status

When to use

Use this task to check the status of all GUI web servers (GWSs) status.

Related information

See the following topic in this document:

- "GWSs" (p. 11-9)

Before you begin

Users must manage all distributed GUI web servers simultaneously from the OMS server.

Task

Complete the following steps to check GWS status.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command line to check GWS status:

```
gui_platform_cntrl status
```

Result: The system outputs GWS status.

In a distributed configuration, the status of the OMS server and the status of all configured distributed GUI web servers are displayed.

In the command output, all associated process are listed with their associated pid. A value of `-1` indicates that the associated process is not running.

A value of `na` indicates that the process is not expected to be running. The value of `na` should be displayed for the Apache and tomcat process definitions on the OMS server.

On each distributed GUI web server process, only two running processes are reported: the apache http process and the tomcat process.

END OF STEPS

Allow a Domain for the GUI Web Server

When to use

Use this task to allow a domain or domains for the GUI web server (GWS).

Related information

See the following topic in this document:

- "apache_config command" (p. 11-10)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to allow a domain for the GUI web server.

1 From the machine on which the management system is running, log in as **`root`**.

Result: You are now logged in as **`root`**.

2 Using the command format specified in "apache_config command" (p. 11-10), enter the following command to allow a domain for the GUI web server:

```
/opt/lucent/platform/bin/apache_config -a <domain name>
```

Result: The specified domain is now allowed. For this command to take effect, the GUI web server must be restarted. (If the management system is up and running, use the **gui_platform_cntrl restart** command. If management system is down, use the "Start the Platform" (p. 9-5) task.)

END OF STEPS

View the Domain Allowed for the GUI Web Server

When to use

Use this task to view the domain or domains that are allowed for the GUI web server (GWS).

Related information

See the following topic in this document:

- "apache_config command" (p. 11-10)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view the domain or domains that are allowed for the GUI web server.

1 From the machine on which the management system is running, log in as **root**.

Result: You are now logged in as **root**.

2 Enter the following command to view the allowed domain or domains for the GUI web server:

```
/opt/lucent/platform/bin/apache_config -v
```

Result: A list of allowed domains is displayed.

END OF STEPS

Reconfigure OMS to Add Distributed TNA/CNA

When to use

Use this task to add a distributed TL1 network adapter (TNA) or a distributed CMISE network adapter (CNA).

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed TNA/CNA server must be installed.

If the TNA/CNA application on the distributed server is up and running, it should be brought down.

The following procedure used the term *NA bundle*, which defined as the both the application files and the cron jobs that are associated with the NA.

Task

Complete the following steps to reconfigure OMS to add distributed TNA/CNA.

1 From the co-resident HP® server on which the management system is running, enter the following command lines to add the new distributed NA configuration and to notify the management system of this new distributed NA configuration:

Log in as **root**.

```
/opt/lucent/platform/bin/lt_add_controller
```

Select **TNA** or **CNA**.

Result: The new controller is added and the management system is now notified of the new controller.

2 On the server on which BPM resides, enter the following command line to notify BPM about the new distributed NA configuration:

Log in as **root**.

```
/opt/lucent/platform/bin/lt_add_controller
```

Select **BPM-TNA** or **BPM-CNA**.

Log in as **bpm**.

```
platform_cntrl stop
```

```
platform_cntrl start
```

3 If you have a distributed GWS, enter the following command lines, on each GWS, to notify the GWSs about the new distributed NA configuration:

Log in as **root**.

```
/opt/lucent/install/bin/lt_add_controller
```

Note: Repeatedly select GWS-NA for each distributed CNA or TNA.

4 From the new distributed NA server, enter the following command lines to bring the application up:

Log in as **oms**.

```
platform_cntrl start
```

Result: The management system is now brought up on the new distributed server.

5 For TNA NEs, refer to "Reparent TL1 NEs from TNA to Another TNA" (p. 32-11) to reparent TL1 NEs from co-resident TNA to the distributed TNA.

6 For CMISE NEs, refer to "Reparent CMISE NEs from a CNA to Another CNA" (p. 32-9) to reparent CMISE NEs from co-resident CNA to the distributed CNA.

7 If needed, refer to "Reconfigure OMS to Remove Co-resident TNA/CNA" (p. 11-33) to clean up the co-resident network adaptor.

END OF STEPS

Reconfigure OMS to Remove Distributed TNA/CNA

When to use

Use this task to remove the distributed TNA/CNA.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The co-resident TNA/CNA server must be installed.

Make sure all applications (OMS/BPM/TNA/CNA) are brought down.

Ensure there are no NEs associated with the distributed TNA/CNA.

From GUI Screen> Network Communication Group, ensure there are no network communication groups associated with this network adaptor. If there is any, remove/reparent any NEs associated with the group and then remove the group.

Task

Complete the following steps to remove distributed TNA/CNA.

1 From the BPM server and OMS server, enter the following command lines to remove the distributed NA controller:

Log in as **root**.

```
/opt/lucent/platform/bin/lt_remove_controller
```

Note: Select the BPM-TNA/BPM-CNA and TNA/CNA to be removed. If the specific TNA/CNA is not displayed on the remove list, there are NEs/NCGs that are still associated with this NA. All associations must be cleaned up before removing the NA.

2 From the distributed TNA/CNA server, enter the following command lines to bring the TNA/CNA application down:

Log in as **oms**.

```
platform_cntrl stop
```

Result: The TNA/CNA server is brought down.

END OF STEPS

Reconfigure OMS to Add Co-resident TNA/CNA

When to use

Use this task to add a co-resident TL1 network adaptor (TNA) or a co-resident CMISE network adaptor (CNA).

Related information

See the following topics in this document:

- “NAs” (p. 11-2)
- “Reconfigure OMS between Co-resident and Distributed Configuration” (p. 11-13)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to reconfigure OMS to add co-resident TNA/CNA.

1 On the co-resident OMS server, use the following command to check if TNA/CNA bundle is installed:

Log in as **`root`**.

```
/opt/lucent/platform/bin/omsregistry--features OMS
```

Note: If TNA/CNA is in the output list, TNA/CNA is installed.

2 If above checking shows that TNA/CNA bundle is installed, skip to Step 6.

If above checking shows that TNA/CNA bundle is not on the OMS server, continue to Step 3.

3 From the OMS server, enter the following command lines to bring the application down:

Log in as **`oms`**.

```
platform_cntrl stop
```

Result: The application is brought down.

4 On OMS server, enter the following command to add TNA/CNA application bundle:

- Log in as `root`.
- `/opt/lucent/install/bin/lt_add_bundle`
  Note: Select the bundle that you need to install.
- Use the following command to check the installation status, you cannot move on until this installation is completed:
  `tail -f /var/tmp/auto_installer.log`
  Note: Installation does not complete until you see the message “AUTO INSTALL COMPLETED“.
- Perform all post installation related configuration:
  ```
  /opt/lucent/platform/bin/lt_config
  /opt/lucent/platform/bin/lt_set_area
  ```
- Reinstall service pack

5 From the OMS server, enter the following command lines to bring application up:

Log in as `oms`.

```
platform_cntrl start
```

6 On the server where BPM resides, enter the following command lines to notify BPM about the new NA configuration and restart the BPM application:

- Login in as `root`.
- Enter the following command to check if the new TNA is known to BPM:
  `grep -e 9174 /opt/lucent/bpm/etc/RouterConfig.xml`
  Note: If above command returns any entry matches, then the TNA is known to BPM already, no need to add BPM_TNA.
- Enter the following command to check if the new CNA is known to BPM:
  `grep -e 908 /opt/lucent/bpm/etc/RouterConfig.xml`
  Note: If above command returns any entry matches the same server and port, then the CNA is known to BPM already, no need to add BPM_CNA.
- If the result show that TNA/CNA is already known to BPM, skip to Step 7.
  If the result show that TNA/CNA is not known to BPM, enter the following command:
  `/opt/lucent/platform/bin/lt_add_controller`
  Select BPM-TNA or BPM-CNA.
- Login in as `bpm`
  ```
  platform_cntrl stop
  platform_cntrl start
  ```

7 If you have distributed GWS configuration, on each GWS server, enter the following command line to notify GWS about the new NA configuration:

Login in as **root**.

```
/opt/lucent/install/bin/lt_add_controller
```

Repeatly select GWS-NA for each co-resident CNA or TNA.

8 For TNA NEs, refer to "Reparent TL1 NEs from TNA to Another TNA" (p. 32-11) to reparent TL1 NEs from distributed TNA to the co-resident TNA.

9 For CMISE NEs, refer to "Reparent CMISE NEs from a CNA to Another CNA" (p. 32-9) to reparent CMISE NEs from distributed CNA to the co-resident CNA.

10 If needed, refer to "Reconfigure OMS to Remove Distributed TNA/CNA" (p. 11-28) to remove this distributed NA.

END OF STEPS

Reconfigure OMS to Remove Co-resident TNA/CNA

When to use

Use this task to remove co-resident TNA/CNA.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed TNA/CNA server must be installed.

Make sure all application (OMS/BPM/TNA/CNA) are brought down.

Ensure there are no NEs associated with the co-resident TNA/CNA.

From GUI Screen> Network Communication Group, ensure there are no network communication groups associated with this network adaptor. If there is any, remove/reparent any NEs associated with the group and then remove the group.

Task

Complete the following steps to remove co-resident TNA/CNA.

1 From the co-resident HP server and from the BPM server, enter the following command to remove the co-resident controller.

Log in as **`root`**.

```
/opt/lucent/platform/bin/lt_remove_controller
```

Note: Select the co-resident TNA/CNA and/or BPM-TNA/BPM-CNA to be removed. If the co-resident TNA/CNA is not displayed on the remove list, there are NEs that are still associated with this NA. All associations must be cleaned up before removing the NA.

2 After all NCGs for the co-resident TNA/CNA are moved and are working properly on the newly distributed NAs, bring down the application:

On the co-resident management system server, log in as **`tna`** or **`cna`**.

```
platform_cntrl stop
```

3 Enter the following command lines to remove the NA bundle from the co-resident server.

On the management server, log in as **`root`**

```
/opt/lucent/install/bin/lt_remove_bundle [TNA | CNA]
```

When running the **`lt_remove_bundle`** command, you must select option 2 rather than option 1 and must then again select the **`TNA`** or **`CNA`** bundle for removal. Refer to the "The lt_remove_bundle command" (p. 11-14) for the complete dialog that occurs with the command output that is associated with this command.

END OF STEPS

Reconfigure OMS to Add Distributed BPM Module

When to use

Use this task to add the distributed Bulk Performance Monitoring (BPM) module.

Related information

See the following topics in this document:

- "BPM" (p. 11-6)
- "OMS_BPM license" (p. 5-4)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed BPM server must be completely installed.

The distributed PM server only supports bulk mode collection; therefore, make sure you have "OMS_BPM license" (p. 5-4) before you start.

If the BPM application is running on the distributed server, it must be brought down.

Task

Complete the following steps to reconfigure OMS to add distributed BPM module.

1 From the HP® servers on which the TNA or CNA or NMA is running, enter the following command lines to add the new distributed BPM configuration and to notify the TNA or CNA of this new distributed BPM configuration:

Log in as **root**.

```
/opt/lucent/platform/bin/lt_add_controller
```

Select **BPM**.

> **Result:** The new controller is added and the management system is now notified of the new controller.

2 The distributed PM server only supports bulk mode collection; therefore, if you have not installed the bulk mode license, use the "Add a License" (p. 5-18) task to add the "OMS_BPM license" (p. 5-4) now.

3 From the co-resident HP® server on which the management system is running, log in as **oms** and enter the following command lines to restart application and GUI:

```
platform_cntrl stop

platform_cntrl start
```

4 From the co-resident HP® server on which the management system is running, enter the following command lines to bring the BPM module down:

Log in as **bpm**.

```
platform_cntrl stop
```

Result: The BPM module is brought down.

5 If old BPM data doesn't need to be migrated, go directly to step 13. If old BPM data needs to be migrated, do the following. From the co-resident HP® server on which the management system is running, log in as **bpm** and enter the following command lines to put BPM tablespace in read-only mode:

```
sqlplus bpmdba/dbmanager

alter TABLESPACE BPM_USER_DATA read only;

alter TABLESPACE CONFIGURATION_DATA  read only;

alter TABLESPACE PERSISTENT_DATA read only;

alter TABLESPACE TEMPORARY_DATA read only;

alter TABLESPACE CONFIGURATION_INDEX read only;

alter TABLESPACE PERSISTENT_INDEX read only;

alter TABLESPACE TEMPORARY_INDEX read only;

exit
```

6 As the BPM user on the co-resident server, enter the following command line to change directories and export database data:

```
mkdir /backups/bpm

cd /backups/bpm

exp bpm/dbmanager owner=bpm file=expbpm.dmp log=/tmp/expbpm.log
```

7 As the BPM user on the co-resident, enter the following command lines to FTP the **expbpm.dmp** file to the distributed BPM machine:

```
ftp <ip_of_distributed_bpm_server>
```

Enter the BPM user ID and password.

```
ftp> mkdir /backups/bpm

ftp> cd /backups/bpm

ftp> put expbpm.dmp

ftp> quit
```

8 On the distributed BPM server, log in as `root` and enter the following command line to put the platform in maintenance mode:

```
su - oms -c "platform_cntrl begin_maintenance"
```

9 On the distributed BPM server, enter the following command line to start the cache database:

```
/opt/lucent/oracle/oracle_start -s bpm
```

10 As an **oracle** user on the distributed BPM server, enter the following command lines:

```
cd ~bpm

. ./.profile

 sqlplus bpmdba/dbmanager @/opt/lucent/bpm/oracle/tablespace.sql
```

You are now left in an SQLPLUS session. Enter the following command line to quit the session:

```
exit
```

11 As a **bpm** user on the distributed BPM server, enter the following command lines:

```
cd /backups/bpm

imp bpm/dbmanager Full=y file=expbpm.dmp log=/tmp/impbpm.log
```

Result: The following warning is displayed. Ignore this warning.

```
IMP-00015: following statement failed because the object
already exists: "CREATE procedure drop_object ( p_name IN
varchar2, p_type varchar2 , p_othe"
```

12 On the distributed BPM server, enter the following command lines to stop Oracle:

On the distributed server, log in as **root**.

```
/opt/lucent/oracle/oracle_stop
```

```
su - oms -c "platform_cntrl end_maintenance"
```

13 On the distributed BPM server, enter the following command lines to bring the BPM module up:

On the distributed server, log in as **oms**.

```
platform_cntrl start
```

14 Use the following method to verify that BPM is running in bulk mode and is communicating correctly:

Log in as **bpm**.

```
dsp "sysparams where name = 'OMS_BPM'"
```

Result: If the returned output is `no rows selected`, the distributed BPM did not establish communication correctly or BPM is running in TP-mode. If OMS_BPM value is Ø, BPM is running in bulk mode, go to next step.

15 If PM collection is not enabled yet, do the following:

1. Enable the PM collection from GUI
2. Wait for at least 30 minutes
3. Go to Step 16

16 Enter the following command lines to validate that BPM is collecting data.

On the distributed server, log in as **bpm**.

```
dsp "count(*)" node15m
```

```
dsp "count(*)" node24h
```

Result: If the 15 minute collection is enabled, the 15 minute logs are updated every 15 minutes. If 24 hour collection is enabled, the 24 hour logs are updated daily.

17 Go to "Reconfigure OMS to Remove Co-resident BPM module" (p. 11-41) to cleanup co-resident BPM module.

END OF STEPS

Reconfigure OMS to Remove Distributed BPM Module

When to use

Use this task to remove the distributed Bulk Performance Monitoring (BPM) module.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The co-resident BPM server must be installed.

The co-resident PM server only support TP mode collection; therefore, make sure you have "OMS_BPM license" (p. 5-4) before you start.

Task

Complete the following steps to remove distributed BPM.

1 From the distributed BPM server, enter the following command lines to bring the BPM application down:

Log in as **oms**.

```
platform_cntrl stop
```

Result: The BPM server is brought down.

2 On the co-resident server and on all distributed GWS/TNA/CNA servers, enter the following command line:

Login in as **root**.

Edit /etc/hosts and remove this distributed BPM hostname from the file.

Result: This distributed BPM module is removed.

END OF STEPS

Reconfigure OMS to Remove Co-resident BPM module

When to use

Use this task to remove co-resident BPM module.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed BPM server must be installed.

The distributed PM server only support bulk mode collection; therefore, make sure you have "OMS_BPM license" (p. 5-4) before you start.

Task

Complete the following steps to remove co-resident BPM.

1 From the co-resident BPM server, enter the following command lines to bring the BPM application down:

Log in as **bpm**.

```
platform_cntrl stop
```

2 Enter the following command lines to remove the BPM bundle from the co-resident server.

On the management server, log in as **root**

```
/opt/lucent/install/bin/lt_remove_bundle BPM
```

When running the **lt_remove_bundle** command, you must select option 2 rather than option 1 and must then again select the **BPM** bundle for removal. Refer to the "The lt_remove_bundle command" (p. 11-14) for the complete dialog that occurs with the command output that is associated with this command.

END OF STEPS

Reconfigure OMS to Add Distributed GUI Web Server

When to use

Use this task to add the distributed GUI.

Related information

See the following topics in this document:

- "OMS_GWS license" (p. 5-8)
- "GWSs" (p. 11-9)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed GWSs must be installed.

Task

Complete the following steps to reconfigure OMS to add distributed GUI web server.

1 On the co-resident server, enter the following command lines to add all new distributed GWS information.

On the co-resident server, log in as **`root`**.

```
/opt/lucent/platform/bin/lt_add_controller
```

Select **GWS** and enter the required information.

Result: The GUI daemon automatically restarts to read the GUI configuration file, which is **/etc/opt/lucent/gws.cfg**.

2 From the co-resident HP® server on which the management system is running, enter the following to stop the co-resident GWS:

Log in as **`oms`**.

```
gui_platform_cntrl stop_local
```

Result: The co-resident GWS is stopped.

3 From the co-resident HP® server on which the management system is running, enter the following to start all distributed GWSs:

```
gui_platform_cntrl start
```

Result: The GWSs have been started.

4 From the co-resident HP® server on which the management system is running, enter the following command line to validate the status of the GWS:

```
gui_platform_cntrl status
```

END OF STEPS

Reconfigure OMS to Remove Distributed GUI Web Server

When to use

Use this task to remove the distributed GUI web server.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The co-resident GUI web server must be installed.

Task

Complete the following steps to remove distributed GUI web server.

1 On distributed GUI web server, enter the following command lines to make sure distributed GWS application is not running on the server:

Log in as **oms**.

```
gui_platform_cntrl stop
```

2 On co-residnet server, enter the following command lines:

Log in as **root**.

Note: Make sure this distributed GWS server name is not in **/etc/opt/lucent/GWS.cfg**.

3 If GWS.cfg ever need to be modified, enter the following command lines to restart the GUI daemon:

```
/opt/lucent/platform/bin/gui_platform_startup_rc restart
```

Note: Wait till GUI daemon restarts.

4 Edit /etc/hosts and remove the distributed GWS hostname from the file.

Result: This distributed GUI web server is removed.

END OF STEPS

Reconfigure OMS to Add Co-resident GUI Web Server

When to use

Use this task to add a co-resident GUI web server (GWS).

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The co-resident GWS server must be installed.

If the GUI application on the distributed server is up and running, it should be brought down.

Task

Complete the following steps to reconfigure OMS to add co-resident GUI web server.

1 On the co-resident OMS server, use the following command to make sure GUI is installed:

Log in as **`root`**.

```
/opt/lucent/platform/bin/omsregistry --features OMS
```

Note: If GWS is in the output list, GUI is installed.

2 If GUI is available on the co-resident OMS server, go to Step 7.

3 From the OMS server, enter the following command lines to bring the application down:

Log in as **`oms`**.

```
platform_cntrl stop
```

Result: The GUI web server is brought down.

4 On OMS server, enter the following command to add GWS application bundle:

- Log in as `root`.
- **`/opt/lucent/install/bin/lt_add_bundle`**
  Note: Select the GWS bundle that you need to install.
- Use the following command to check the installation status, you cannot move on until this installation is completed:
  `tail -f /var/tmp/auto_installer.log`
  Note: Installation does not complete until you see the message “AUTO INSTALL COMPLETED“.
- Reinstall service pack

5 On the co-resident OMS server, enter the following command to bring application up:

Log in as `oms`.

```
platform_cntrl start
```

6 On the co-resident OMS server, enter the following command line to bring all distributed GUI down:

Log in as `oms`.

```
gui_platform_cntrl stop
```

7 On the co-resident OMS server, enter the following command lines to clear out all distributed GWS information and restart GUI daemon processes:

- Login in as `root`.

-
  ```
  cd /etc/opt/lucent
  cp -p gws.cfg gws.cfg.old
  > /etc/opt/lucent/gws.cfg
  /opt/lucent/platform/bin/gui_platform_startup_rc restart
  ```
  Note: Wait till GUI daemon restart.

8 On the co-resident OMS server, enter the following command to bring up the GUI again:

Log in as `oms`

```
gui_platform_cntrl start
```

9 On the OMS server, enter the following command lines to validate GUI web server status:

Login in as **`oms`**.

```
gui_platform_cntrl status
```

Result: The GUI is running from the co-resident server.

10 Launch the OMS GUI from co-resident GUI.

Result: The OMS GUI is launched.

END OF STEPS

Reconfigure OMS to Disable Co-resident GUI Web Server

When to use

Use this task to disable co-resident GUI Web server.

Important! It is not recommended to remove co-resident GWS, the copy of GUI can be used for backup purpose.

Related information

See the following topics in this document:

- "NAs" (p. 11-2)
- "Reconfigure OMS between Co-resident and Distributed Configuration" (p. 11-13)

Before you begin

The distributed GWS module must be installed and configured.

Task

Complete the following steps to disable the co-resident GUI web server.

1 On the co-resident OMS server, enter the following command lines to bring the co-resident GUI down:

Log in as **oms**.

```
gui_platform_cntrl stop_local
```

Result: The GUI is brought down on the co-resident server.

END OF STEPS

12 Resource Monitor

Overview

Purpose

This chapter contains the conceptual information and needed tasks to support the Resource Monitor.

Contents

Resource Monitor Concepts

Resource Monitor defined

The Resource Monitor is a management system feature that executes periodic checks on the mounting of the file system and the usage of the file system, and the swap space. The Resource Monitor is launched as a Common Object Resource Broker Agent (CORBA™) process and operates with or without the presence of a fault manager (FM).

Resource Monitor supported platforms

The Resource Monitor is supported on the *Server Platforms*.

The Resource Monitor is not supported on the *PC Platform* because it is tailored to HP-UX resource measurements. The PC Platform makes periodic checks of essential disk spaces and performs the needed housekeeping functions for log files via cron jobs.

Resource Monitor checks

The Resource Monitor checks the following areas:

- *File system mounts*
- *File system usage*
- *INODE usage*
- *Swap usage*
- *LAN errors*

Each check that the Resource Monitor performs occurs in a designated number of seconds as defined by the threshold parameter variable.

Resource Monitor alerts

If an error occurs, the Resource Monitor alerts the console device and the system log file. Internal system errors are sent to the process log file. Also, if the Resource Monitor detects that a fault manager exists, the condition is raised to a platform alarm.

When an error condition is cleared, a clear message is sent to the console device, the system log file, and the fault manager (if relevant).

Threshold changes

The Resource Monitor threshold parameter variables should not be changed; however if they are changed, the platform must be restarted so the changes take affect.

Resource Monitor related platform alarms

The following hot links provide additional information on platform alarms that could be related to the malfunctioning of the Resource Monitor:

- "FS_INODES_LOW" (p. 42-16)
- "FS_INODES_WARNING" (p. 42-17)
- "FS_SPACE_LOW" (p. 42-17)
- "FS_SPACE_WARNING" (p. 42-18)
- "FS_UNMOUNTED" (p. 42-18)

The following hot links provide additional information on platform alarms that are related to LAN errors:

- "ETHER_COLLISION" (p. 42-15), for the HP® server on which the management system resides only
- "ETHER_ERROR" (p. 42-15), for the HP® server on which the management system resides only

Verify that all HPFSs Are Mounted

When to use

Use this task to verify that all High Performance File Systems (HPFSs) listed in the **/etc/fstab** file are mounted.

Related information

See the following topic in this document:

- "Resource Monitor Concepts" (p. 12-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to verify that all HPFSs listed in the **/etc/fstab** file are mounted.

1 From the machine on which the management system is running, log in as **root**.

2 At the prompt, enter the following command to mount the file system:

```
mount /Mount
```

Result: The following events should occur:

- A LOG_EVENT type message is sent to the system-wide log file to indicate that the file system is no longer mounted.
  Example:
  ```
   011016140658+0100:7830-19:LOG_EVENT:resource_
  mon:ResourceMonitorProcs.C:266:
  Filesystem /Mount is not mounted
  ```
- A message is sent to the system console to indicate the alert condition.
  Example:
  ```
  Filesystem /Mount is not mounted
  ```
- Assuming the presence of a fault manager, an alarm is raised indicating the alert condition.

3 To remount the file system, enter the following command at the prompt:

```
mount -a
```

Result: The following events should occur:

- A `LOG_EVENT` type message is sent to the system-wide log file to indicate that the alert condition has been cleared.
  Example:
  ```
   011122155709+0000:4044-19:LOG_EVENT:resource_
  mon:ResourceMonitorMain.C:346: Filesystem/Mount: unmounted
  condition cleared
  ```
- A message is also sent to the system console to indicate the cleared alert condition.
  Example:
  ```
  Filesystem/Mount: unmounted condition cleared
  ```
- The fault management alarm for this alert should disappear.

The verification of the mounting of all HPFSs should now be completed.

END OF STEPS

Change the CPU Usage Monitor Alert Threshold

When to use

Use this procedure to change the CPU usage monitor alert threshold.

Related information

See the following topic in this document:

- "Resource Monitor Concepts" (p. 12-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to change the CPU usage monitor alert threshold.

1 From the machine on which the management system is running, log in as **root**.

2 At the prompt, enter the following command to change directories:

```
cd /opt/lucent/oms/etc
```

3 Make a copy of the **resource_mon.cfg** file so a backup exists:

```
cp resource_mon.cfg resource_mon.cfg.ori
```

4 Use the **vi** editor to access the **resource_mon.cfg** file:

```
vi resource_mon.cfg
```

5 Search for the line containing the string `RM_CPU_LIMIT`.

6 Change the default value/value that is currently in effect for the RM_CPU_LIMIT. (Note that the value is a percentage from 1% to 100%.)

7 Use the following command to save the changes and exit the file:

```
<shift> ZZ
```

Result: The default value in the **resource_mon.cfg** file has been changed.

END OF STEPS

13 Logs

Overview

Purpose

This chapter contains conceptual information and related tasks for the logs that are available with the management system.

Contents

Log Concepts

Available management system logs

The logs that are offered as the suite of management system logs include the following:

- TL1 Alarm Log (AEL)
- Alarm Log
- NE Command and Response Log (CRL)
- NE Notification Log (NEL)
- Security Log (SEL)
- User Activity Log (UAL)
- Protection Switch Event (PSE) Log
- Threshold Crossing Alert (TCA) Log

These logs are controlled by a set of Fault Management and Log Management installation parameters; refer to "lt_param_reconfig and its menu options" (p. 6-2) for a list of hot links; each hot link points to details about the particular installation parameter. In addition, refer to "Log Management Variables" (p. 6-12) for details on each installation parameter.

In addition, refer to the "Security Log" (p. 13-2) section in this document for details on the Security Log; refer to the *OMS Network Element Management Guide* for details on the T1 Alarm Log, the Command and Response Log, the NE Notification Log, the User Activity Log, and the Protection Switch Event Log; refer to the *OMS Service Assurance Guide* for details on the Alarm Log and the Threshold Crossing Alert (TCA) Log.

Security Log

The Security Log, which is one of the suite of logs that the management system offers, includes details of all security-related activities, including these system and user-initiated activities:

- All management system login events, such as log ins, log outs, creation of users accounts, deletion of user accounts, and password changes.
- All user-initiated events that result in network or NE configuration changes.

The Security Log is enabled or disabled upon the installation of the management system with the "Enable Security Log" (p. 6-12) installation parameter. The setting of the "Security Log Retention Time Period" (p. 6-12) installation parameter controls the record keeping and retention periods involved with the log records.

Only users who have the Security Log task in their user role profile can access the Security Log. See the "Security Log user task" (p. 7-21) for details.

For details on how to view the security log, see the "View a List of a Security Log Records" (p. 13-4) and the "View the Details of a Security Log Record" (p. 13-5) tasks.

For more information about management system logs, including information about retention time for log entries, see the *OMS Network Element Management Guide*.

Log related platform alarms

The following hot links provide additional information on platform alarms that are related to logs:

- "ALARMS_LOG_SPACE_LOW" (p. 42-7)
- "ALARMS_LOG_SPACE_VERY_LOW" (p. 42-8)
- "CR_FULL" (p. 42-9)
- "CR_NEARLY_FULL" (p. 42-10)
- "CR_FULL" (p. 42-9)
- "FLAPPING_ALARMS_DETECTED" (p. 42-16)

- “LOG_FILES_HAVE_BEEN_TRIMMED” (p. 42-19)
- “NEL_FULL” (p. 42-21)
- “NEL_NEARLY_FULL” (p. 42-22)
- “PID_DATA_SIZE” (p. 42-22)
- “PID_DEACTIVATED” (p. 42-23)
- “PID_STACK_SIZE” (p. 42-23)
- “SL_FULL” (p. 42-25)
- “SL_NEARLY_FULL” (p. 42-26)
- “UTL_FULL” (p. 42-27)
- “UTL_NEARLY_FULL” (p. 42-27)

View a List of a Security Log Records

When to use

Use this task to view a list of Security Log records.

Related information

See the following topics in this document:

- "Security Log" (p. 13-2)
- "View the Details of a Security Log Record" (p. 13-5)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view a list of Security Log records.

1 Use the icons or the object list to follow this path:

- **Logs > Security Log**

  Result: The Search for security logs page is displayed.

2 Specify the criteria for your search by making selections in the search fields and click the **Search** button.

  Result: The Security Logs page is populated with entries that meet your search criteria.

END OF STEPS

View the Details of a Security Log Record

When to use

Use this task to view the details of a Security Log record.

Related information

See the following topic in this document:

- "Security Log" (p. 13-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view the details of a Security Log record:

1. Use the icons or the object list to follow this path:

   - **Logs > Security Log**

   Result: The Search for security logs page is displayed.

2. Specify the criteria for your search by making selections in the search fields and click the **Search** button.

   Result: The Security Logs page is populated with entries that meet your search criteria.

3. To view the details of a specific log entry, click the details button next to the log entry.

   Result: The details of the selected log entry are displayed below the table.

END OF STEPS

14 Logs Extraction

Overview

Purpose

This chapter provides the concepts that are needed to understand and the tasks that are needed to run the Logs Extraction tool.

Contents

Logs Extraction Concepts

Logs Extraction definition

The Logs Extraction tool is a licensed feature of the management system that enables users to extract logs from the management system database table to a corresponding file for archiving purposes. The management system will purge the aged logs from these tables according to the configured retention period of each table. Users can use this Logs Extraction tool to archive the aged logs before purging.

The Logs Extraction is supported for the following management system database tables:

- User Security Logs; also refer to "Enable Security Log" (p. 6-12)
- User Activities Logs; also refer to "Enable User Activity Log" (p. 6-13)

- NE Command-Response Logs; also refer to "Enable Command Response Log" (p. 6-15)
- NE Notification Logs; also refer to "Enable NE Notification Log" (p. 6-14)

Logs Extraction supported platforms

Logs Extraction is supported on the *Server Platforms* and the *PC Platform*.

Logs Extraction licensing

The Logs Extraction tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Logs Extraction modes of execution

Logs Extraction can be executed through the following modes:

- On-demand via the command line by executing the tool; refer to the "On-Demand Execution of Logs Extraction" (p. 14-7) task for details.
- Scheduled via a cron job; refer to the "Schedule Automatic Logs Extraction" (p. 14-9) task for details.

Logs Extraction Output Files

Data Files

This Logs Extraction tool produces a set of **.gz** data files each corresponding to a logs table. The **.gz** files are located in the following directories:

```
/var/opt/lucent/data_extraction/KEEPLOGS/securitylog/<.gz files>
```

```
/var/opt/lucent/data_extraction/KEEPLOGS/useractivitylog/<.gz files>
```

```
/var/opt/lucent/data_extraction/KEEPLOGS/cmdrsplog/<.gz files>
```

```
/var/opt/lucent/data_extraction/KEEPLOGS/nenotificationlog/<.gz files>
```

The file name has the format below:

```
<hostname>.<datetimestamp>.OMS.<log table>.xls.gz
```

For space saving purposes, the files are gzipped into **.gz** files. The **.gz** files could be converted to **.xls** by:

gunzip <.xls filename>

Note: The **.gz** files are created one file per log table per day. If the same logs table is extracted multiple times in the same day, the earlier **.gz** file will be overridden, even when the subsequent extractions select different logged intervals.

Traces file

The traces of each run of Logs Extraction are accumulated in the following file:

```
/var/opt/lucent/data_extraction/KEEPLOGS/keeplogs_traces.log
```

Edit keeplogs.properties to Customize Logs Extraction

When to use

Use this task to change variables in the following **keeplogs.properties** file in order to customize Log Extraction.

/opt/lucent/oms/bin/keeplogs.properties

Editable Variables

Nine editable variables along with the defaults are listed:

1. Output the **.gz** files to this root directory
   REPORTDIR=**/var/opt/lucent/data_extraction/KEEPLOGS**
2. Output the trace file to this directory
   LOGDIR=**/var/opt/lucent/data_extraction/KEEPLOGS**
3. Keep **.gz** files for this number of days
   RETENTION_DAYS=**31**
4. Extract this log table(s) when no log table is specified at the command-line. Possible values are: **sec**, **ual**, **cr**, **nl**, **alllogs** which stand for securitylog, useractivitylog, cmdrsplog, and nenotificationlog, respectively.
   WHICHLOG=**sec**
5. Extract data logged during this date or period. Possible values: **YYYYMMDD**, **alldays**, **hours**.
   YYYYMMDD indicates that only data of the target tables logged during this particular date will be extracted; **alldays** indicates that all data of the target tables logged will be extracted; **hours** indicates that only data of the target table(s) logged during the past **Nx24 hours** will be extracted, where **N** is defined by **SEC_DAYS**, **UAL_DAYS**, **CR_DAYS** or **NL_DAYS**.
   WHICHDATE=**hours**

   Attention!

   - Variables **SEC_DAYS**, **UAL_DAYS**, **CR_DAYS**, and **NL_DAYS** will be ignored when **YYYYMMDD** or **alldays** is selected.
   - For logs extraction cron jobs of **Daily/Weekly/Monthly** periodic frequency, set the corresponding **SEC_DAYS**, **CR_DAYS**, and/or **NL_DAYS** to proper values so that the new data logged during each period will be extracted. That is, 1 for **Daily**, 7 for **Weekly**, and 31 for **Monthly**, while WHICHDAY= **hours**.
6. When **hours** is selected as the logged period, **SEC_DAYS** times 24 determines the passed number of hours of logged data to be extracted from the **securitylog** table.
   SEC_DAYS=**1**

7. When **hours** is selected as the logged period, **UAL_DAYS** times 24 determines the passed number of hours of logged data to be extracted from the **useractivitylog** table.
   ```
   UAL_DAYS=1
   ```
8. When **hours** is selected as the logged period, **CR_DAYS** times 24 determines the passed number of hours of logged data to be extracted from the **cmdrsplog** table.
   ```
   CR_DAYS=1
   ```
9. When **hours** is selected as the logged period, **NL_DAYS** times 24 determines the passed number of hours of logged data to be extracted from the **nenotificationlog** table.
   ```
   NL_DAYS=1
   ```

Note: The values in this **keeplogs.properties** file only take effect when they are not entered at the command-line. Otherwise, those values at the command-line will take precedence.

Related information

See the following topics in this document:

- "Logs Extraction Concepts" (p. 14-1)
- "On-Demand Execution of Logs Extraction" (p. 14-7)
- "Schedule Automatic Logs Extraction" (p. 14-9)
- "Disable Automatic Logs Extraction" (p. 14-12)

Before you begin

The Logs Extraction must not be running on-demand or scheduled to avoid unexpected behavior.

Task

Complete the following steps to edit the **keeplogs.properties** file in order to customize Logs Extraction.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command to change directories:

```
cd /opt/lucent/oms/bin
```

3 Enter the following command to invoke the vi editor and to edit the **keeplogs.properities** file:

```
vi keeplogs.properties
```

4 Change one or more variables to other possible values to fit your needs. Refer to "Editable Variables" (p. 14-4) for the possible values.

5 Enter the following command to save the changes made to the file and to exit the file:

```
<Shift> ZZ
```

Result: The **keeplogs.properities** file has been changed in order to customize the Logs Extraction.

END OF STEPS

On-Demand Execution of Logs Extraction

When to use

Use this task to perform an on-demand execution of the Logs Extraction command-line tool.

Related information

See the following topics in this document:

- "Logs Extraction Concepts" (p. 14-1)
- "Edit keeplogs.properties to Customize Logs Extraction" (p. 14-4)

Before you begin

Ensure the **Oracle** platform is up and running.

Consider which logs table(s) and which logged interval to extract; prepare to specify them on the command-line or in **keeplogs.properties** file. Otherwise, the **securitylog** data logged during the past 24 hours will be extracted as default.

If the Logs Extraction of a particular log is already run at an earlier time of the day, and the output files are still in the output directories, port the files to a permanent place or rename the files to prevent overriding.

Task

Complete the following steps to run the Logs Extraction command-line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 To execute the tool, enter the following command with or without input parameter(s):

```
KeepLogs {YYYYMMDD| alldays | hours } {sec | ual | cr | nl |
alllogs }
```

The input parameters share the same values as those defined in **keeplogs.properties** file. Refer to "Editable Variables" (p. 14-4) for the explanation of the values.

3 To verify the tool ran successfully, view the traces file in:

```
/var/opt/lucent/data_extraction/KEEPLOGS/keeplogs_traces.log
```

4 To verify the data are extracted properly, view the output files in:

```
/var/opt/lucent/data_extraction/KEEPLOGS/*/*.gz
```

5 Optionally, port the **.gz** files and the trace files to a permanent storage location.

END OF STEPS

Schedule Automatic Logs Extraction

When to use

Use this task to schedule an automatic execution of the Logs Extraction command-line tool through the use of a cron job.

Related information

See the following topics in this document:

- “Logs Extraction Concepts” (p. 14-1)
- “Edit keeplogs.properties to Customize Logs Extraction” (p. 14-4)
- “Disable Automatic Logs Extraction” (p. 14-12)

Before you begin

Ensure the **Oracle** platform is up and running at the scheduled run time.

There will be no input parameters to enter on the command line for a cron job. The default is to extract the **securitylog** data logged during the past 24 hours. If other table or interval is desired, edit **keeplogs.properties** for the changes.

If the Logs Extraction of a particular log is already run at an earlier time of the day, and the output files are still in the output directories, port the files to a permanent place or rename the files to prevent overriding.

Task

Complete the following steps to schedule the automatic execution of the Logs Extraction command-line tool.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **6**, which is Logs Extraction, and press **Enter**.

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To enable the automatic execution of the tool, select **Option 1** and press **Enter** to review the cronjobs.

Result: The default values for the automatic tool execution are shown. The default execution time is *1:00* A.M. and the default frequency is *daily*.

5 If the values shown are acceptable, go to Step 10 to save the changes.

To change the execution time, go to Step 6.

To change the frequency of execution, go to Step 8.

6 To change the execution time from the time shown, enter **1** and press **Enter**.

7 Enter the new time in 24-hour format (for example: 09:00 for 9:00 A.M. and 21:30 for 9:30 P.M.) and press **Enter**.

Result: The newly specified time value is displayed.

8 To change the frequency of execution, enter **2** and press **Enter**.

Result: The frequency options are displayed.

9 Select a frequency among the following:

- If you select **Daily**, go to Step 10.
- If you select **Weekly**, select a day of the week and press **Enter**.
- If you select **Monthly**, select a date of the month and press **Enter**.
- If you select **Fixed Date**, enter the month number (1 through 12), a dash (-), a date of the month (1 through 31) and press **Enter**.

Attention! To extract the new data logged during each period, in **keeplogs.properties**, set `WHICHDAY=`**`hours`**, and the corresponding **SEC_DAY**, **UAL_DAYS**, **CR_DAYS**, and/or **NL_DAYS** to `1` for **`Daily`** frequency, `7` for **`Weekly`** frequency, and `31` for **`Monthly`** frequency.

10 To save any changes made, enter **s** and press **Enter**.

Result: Changes made to the automatic execution of the tool are saved and the automatic execution of the tool is scheduled.

11 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the Logs Extraction command-line tool is completed.

END OF STEPS

Disable Automatic Logs Extraction

When to use

Use this task to disable the automatic execution of the Logs Extraction command-line tool.

Related information

See the following topics in this document:

- "Logs Extraction Concepts" (p. 14-1)
- "Edit keeplogs.properties to Customize Logs Extraction" (p. 14-4)
- "Schedule Automatic Logs Extraction" (p. 14-9)

Before you begin

Make sure the tool is not running either on-demand or scheduled to prevent unexpected behavior.

Task

Complete the following steps to disable the automatic execution of the Logs Extraction command-line tool.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **6**, which is Logs Extraction, and press **Enter**:

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed.

5 Select the tool to be disabled and press **Enter.**

Result: A confirmation is displayed to verify that you want to disable the execution of this particular tool.

6 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the Logs Extraction command-line tool is disabled.

END OF STEPS

15 One Vision Daily Log Extraction

Overview

Purpose

This chapter provides the concepts and the tasks that are needed to run the One Vision Daily Log Extraction tool.

Important!This is a licensed feature and is available to the user if it has been licensed for the customer.

Contents

One Vision Daily Log Extraction Concepts

One Vision Daily Log Extraction definition

The One Vision Daily Log Extraction tool is a licensed feature of the management system that have the following functionalities:

- Runs automatically each day at a fixed time.
- Extracts user activity log and security log data from the native application database for a 24 hour period.
- Generates a single file report for all user activities, defined in the common set of user activity actions, that conforms to the OneVision user activity log report file format.
- Converts individual user activity log entries from the management system native databases into the format of the associated One Vision common user activity log message.

- Filters out all native management system user activity log entries that are not part of the OneVision set of common user activity log entries.
- Prevents the associated management system file system from exceeding space limits.
- Allows FTP access of generated logs.

The One Vision Daily Log Extraction is supported for the following management system database tables:

- User Security Logs; also refer to "Enable Security Log" (p. 6-12)
- User Activities Logs; also refer to "Enable User Activity Log" (p. 6-13)

One Vision Daily Log Extraction supported platforms

One Vision Daily Log Extraction is supported on the *Server Platform* and the *PC Platform*.

One Vision Daily Log Extraction licensing

The One Vision Daily Log Extraction tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

One Vision Daily Log Extraction modes of execution

One Vision Daily Log Extraction can be executed through the following modes:

- On-demand via the command line by executing the tool; refer to the "Run oneVisionExtractLogs for On-Demand Logs Extraction script" (p. 15-10) task for details.
- Scheduled via a cron job; refer to the "Run lt_cronadmin to enable or disable the oneVisionExtractLogs script" (p. 15-7) task for details.

One Vision Daily Log Extraction Directories and Files

OneVisionConfig script

This OneVisionConfig script prompts the user to enter configuration parameters for OneVisionExtractLogs script. The OneVisionConfig script files are located in the following directory:

`/opt/lucent/oms/bin/oneVisionConfig`

lt_cronadmin script

This lt_cronadmin script is used to schedule the daily execution of the oneVisionExtractLogs script. The lt_cronadmin script files are located in the following directory:

`/opt/lucent/platform/bin/lt_cronadmin`

OneVisionExtractLogs script

This OneVisionExtractLogs script can be either invoked by cron job for scheduled daily execution or for on-demand execution. The OneVisionExtractLogs script files are located in the following directory:

`/opt/lucent/oms/bin/oneVisionExtractLogs`

Output files

This OneVisionExtractLogs script generates an output log file in the following directory:

`/var/opt/lucent/onevision_activitylogs`

Configuration file

This OneVisionConfig script generates a configuration file **oneVisionReport.cfg** in the following directory:

`/var/opt/lucent/USERDATA/OneVisionLogs`

One Vision Daily Logs Extraction tool extracts specific user activity log information from the database over a 24 hour period and stores the extracted information in a flat ASCII file with a specific log file format.

The functionalities of the tool are as follows:

- Each extracted DB record equates to a single OneVision user event and each record is added as a single line in a format specified in the OneVision general record format table.
- All OneVision user events contained in a given log file are ordered in ascending chronological order.
- The maximum size of each log file size is either: 10MB or 100,000 records.
- The file name has the following format:
  `<HOSTNAME>.<YYYY>-<MM>-<DD>.OMS`
  where:
  `<HOSTNAME>` is the short name of OMS host
  `<YYYY>` is the four character year
  `<MM>` is the two character month (01-12)
  `<DD>` is the two character day (01-31), which identifies the day when the 24 hour log extraction commences.
- All OMS log files are stored in the following directory:
  `/var/opt/lucent/ftp/pub/onevision_activitylogs`

OneVision General Record Format

The following table summarizes the general record format of the OneVision Daily logs Extraction tool.

Field	Format	Description
Event Number	00000 - 99999	A numeric value that uniquely identifies each record in a file. The numbering sequence needs to be continued across log files. In order words, the first event number used in any given log file is a value that is 1 greater than the event number of the last log entry in the previously created log file.
Timestamp	YYYY-MM-DDT HH:MM:SSZ	UTC time in Year, month, day, hour, minutes and second format when the associated activity occurred
Username	alpha-numeric string	The user name associated with the user activity/security record
Hostname	alpha-numeric string	The hostname of the management system computer name
One Vision User Event	alpha-numeric string	The name of the OneVision user event
Rate	alpha-numeric string	String representation of the layer rate value. For OneVision user events that are not associated with a rate, this value is left as an empty string (i.e. null).
Event Parameters	<name>=<value>	Event parameters are tab separated name value attribute pairs that are associated with the user event. There may be zero or more name value pairs associated with the event.

Run OneVisionConfig script

When to use

Use this task to enter configuration parameters for both the scheduled daily execution of oneVisionExtractLogs and the on-demand execution of the oneVisionExtractLogs script.

Related information

See the following topic in this document:

- "One Vision Daily Log Extraction Concepts" (p. 15-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to run OneVisionConfig manually and on-demand from the command line.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter

```
oneVisionConfig
```

3 The Script prompts to specify three parameters:

1. **start date:** This parameter is used by the scheduled daily execution of oneVisionExtractLogs. When cron job invokes this script as scheduled daily execution, it only performs 24 hour log extraction for the previous day. However, when the user executes oneVisionExtractLogs script for the first time, the option to specify log extraction from an earlier date is available.
2. **service mode:** This parameter specifies the rate information of the service mode and contains the value of SDH or SONET. The user has to specify the required service mode.
3. **max number of records per daily log file:** This parameter specifies the maximum number of records that can be extracted by oneVisionExtractLogs script.

Result: The oneVisionConfig script is executed.

The following is a sample of how to run oneVisionConfig script:

-
  ```
  Please enter configuration parameters for
  oneVisionExtractLogs.
  Do you want to use yesterday's date=2008-02-13 as start
  date for extracting logs?
  Please enter Y or N =N
  Please enter start date in the form of <YYYY-MM-DD>
  2008-02-11
  startDate=2008-02-11
  ```

-
  ```
  Please select service mode: 1 for SDH and 2 for SONET.
  Please enter 1 or 2 =1
  serviceMode= SDH
  ```

-
  ```
  Is 10000 as max number of extracted logs per day OK?
  Please enter Y or N =N
  Please enter a number 3000
  maxNumOfRecords=3000
  ```

End of steps

Run lt_cronadmin to enable or disable the oneVisionExtractLogs script

When to use

Use this task to schedule an automatic execution of the oneVisionExtractLogs script through the use of a cron job.

Related information

See the following topics in this document:

- "One Vision Daily Log Extraction Concepts" (p. 15-1)
- "Run OneVisionConfig script" (p. 15-5)

Before you begin

Ensure the **Oracle** platform is up and running at the scheduled run time.

Run the **oneVisionConfig** script.

Task

Complete the following steps to schedule the automatic execution of the oneVisionExtractLogs script.

1 From the machine on which the management system is running, log in as `root`.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **5**, which is One Vision Daily Logs Extraction, and press **Enter**.

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

The current settings would be **disabled**.

4 To enable the automatic execution of the tool, select **Option 1** and press **Enter** to review the cronjobs.

Result: The default values for the automatic tool execution are displayed. The default execution time is *3:00* A.M. and the default frequency is *daily*.

5 If the values shown are acceptable, go to Step 8 to save the changes.

To change the execution time, go to Step 6.

6 To change the execution time from the time shown, enter **1** and press **Enter**.

7 Enter the new time in 24-hour format (for example: 09:00 for 9:00 A.M. and 21:30 for 9:30 P.M.) and press **Enter**.

Result: The newly specified time value is displayed.

8 To save any changes made, enter **s** and press **Enter**.

Result: Changes made to the automatic execution of the tool are saved and the automatic execution of the tool is scheduled.

9 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the One Vision Daily Logs Extraction script is completed.

10 *Optional.*To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed.

11 Select the tool to be disabled and press **Enter.**

Result: A confirmation is displayed to verify that you want to disable the execution of this particular tool.

12 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the Logs Extraction command-line tool is disabled.

END OF STEPS

Run oneVisionExtractLogs for On-Demand Logs Extraction script

When to use

Use this task to perform an on-demand execution of the oneVisionExtractLogs script.

Related information

See the following topics in this document:

- "One Vision Daily Log Extraction Concepts" (p. 15-1)
- "Run OneVisionConfig script" (p. 15-5)

Before you begin

Ensure the **Oracle** platform is up and running.

Run the **oneVisionConfig** script.

Task

Complete the following steps to run the oneVisionExtractLogs script.

1 From the machine on which the management system is running, log in as **oms**.

2 To execute the tool, enter the following command with or without input parameter(s):

```
oneVisionExtractLogs oneday yyyy mm dd
```

```
oneVisionExtractLogs oneday 2008 02 13
```

The above command line will perform log extraction for the date 2008-02-13.

3 To verify the data are extracted properly, view the output files in:

/var/opt/lucent/onevision_activitylogs directory.

The output file format is:

hostname.2008-02-13.oms

END OF STEPS

16 Data Extraction

Overview

Purpose

This chapter provides the concepts that are needed to understand and the tasks that are needed to run the Data Extraction tool.

Contents

Data Extraction Concepts

Data Extraction definition

The Data Extraction tool is a licensed feature of the management system that enables users to extract equipment, alarm, network element (NE), network connection, performance monitoring (PM), and for certain NEs, link connection data from the management system database through the command-line user interface. This data is stored in field-delimited, predefined flat files that are known as *data files*.

Data Extraction supported platforms

The Data Extraction tool is supported on the *Server Platforms*. The Data Extraction tool is not supported on the *PC Platform*.

Data Extraction license

Data Extraction is an optional, licensable feature that is only available to customers who have purchased the feature and installed its license.

The successful operation of Data Extraction requires the "OMS_DET license" (p. 5-6). Feature licenses are typically installed, and thereby activated, upon the installation of the management system. Any subsequent additions of licenses require the license key and are made with the "Add a License" (p. 5-18) task.

Data Extraction installation parameters

The execution and the functioning of Data Extraction and its data files are controlled through this extensive set of installation parameters and their variables:

- "Enable/Disable DET Report Cron" (p. 6-120)
- "Data Extraction Variables for NE Report" (p. 6-92)
- "Data Extraction Variables for Equipment Report" (p. 6-95)
- "Data Extraction Variables for All Alarm Report" (p. 6-98)
- "Data Extraction Variables for Active Alarm Report" (p. 6-102)
- "Data Extraction Variables for Network Connection Report" (p. 6-106)
- "Data Extraction Variables for PM 24 Hour Report" (p. 6-109)
- "Data Extraction Variables for PM 15 Minute Report" (p. 6-113)
- "Data Extraction Variables for Link Connection Report" (p. 6-116)
- "Number of Retry for Push Mode" (p. 6-120)
- "Retry Interval (Minutes) for Push Mode" (p. 6-121)

Data Extraction execution

Data Extraction can be executed in one of two methods:

- automatically, as a nightly cron job
- manually and on-demand from the command line

When run automatically as a nightly cron job, parameter specifications for the Data Extraction feature are made via installation parameters.

When run manually and on-demand from the command line, some parameter specifications for the feature are made directly from the command line. Any parameter choices made directly on the command line, temporarily override specifications made in the installation parameter settings. This functionality assists those users who, regardless if running the nightly cron job, still need access to various data files during peak hours.

With either execution method, the management system must remain up in order to execute Data Extraction properly.

The automatic running of Data Extraction as a nightly cron job is disabled, by default, for all data files. Automatic running can be turned ON by changing the value in the "Enable/Disable DET Report Cron" (p. 6-120) installation parameter. See the "Modify an Installation Parameter" (p. 6-167) task for instructions. In addition, to avoid scheduling operations simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

Regardless of the setting of the "Enable/Disable DET Report Cron" (p. 6-120) installation parameter, Data Extraction can always be run manually and on-demand from the command line, providing the "OMS_DET license" (p. 5-6) is installed.

Data Extraction directory location

The Data Extraction tool is located in the following directory on the management system HP® server:

/opt/lucent/platform/bin/DataExtraction

Data Extraction and Co-Resident and Distributed Architectures

For Co-Resident and Distributed Architectures, the following guidelines apply to for the Data Extraction tool:

- One Data Extraction tool is **/opt/lucent/platform/bin** and one Data Extraction report directory, which is **/var/opt/lucent/data_extraction**, can exist.
- Data Extraction generates all reports on the co-resident server.
- For distributed configurations with distributed BPM, the Data Extraction tool is available on either the OMS server or the distributed BPM server. The Data Extraction tool can only generate TL1 PM reports on the distributed BPM server and the generated reports always remain in the DET report directory on the distributed BPM server. The Data Extraction tool on OMS server can generate the remaining DET reports. For more details on Bulk Performance Monitoring, refer to "BPM" (p. 11-6).

Data Extraction PUSH and PULL Modes

Two modes to view data

Once launched, Data Extraction affords users these two modes with which to view data:

- PULL mode
- PUSH mode

PULL mode

With its PULL mode, after all Data Extraction data files are generated, Data Extraction enables users to view or download any generated data file by specifying the management system server as the HTTP address on a standard web browser, such as Internet Explorer or Netscape.

Format:

```
http://<hostname>.<domain name>/data_extraction
```

Recommendation: For HP® Serviceguard configurations, we recommend the use of the cluster IP or system logical name for the <hostname>.

Example:

```
http://server123.ho.lucent.com/data_extraction
```

PUSH mode

With its PUSH mode, in addition to the what is provided in PULL mode, Data Extraction enables users to transfer data files automatically from the HP® server on which the management system resides to a remote server via **ftp**.

PUSH mode and its installation parameter settings

After all Data Extraction data files are compiled, Data Extraction determines, by way of its installation parameter settings, if any files need to be PUSHed to a remote server and a different directory.

PUSH mode functions by way of its installation parameter settings. The PUSH mode installation parameters are of the following formats for report type X, which can be a data file for an NE, equipment, all alarms, active alarms, network connections, 15-minute PM data, 24-hour PM data, or link connections:

- DET.X_REMOTE_MACHINE, which specifies the IP address of the remote machine is supplied for report type X.
- DET.X_REMOTE_LOGIN, which specifies a login on the remote machine with access to for report type X.
- DET.X_REMOTE_PASSWORD, which specifies a password on the remote machine with which to access the login for DET.X_REMOTE_LOGIN report type X.
- DET.X_REMOTE_DIRECTORY, which specifies an existing directory on the remote machine with which to access the login for DET.X_REMOTE_LOGIN report type X.

PUSH mode, ftp, report errors, and alarms

Final report files are copied via **ftp** to the remote server. If **ftp** fails, Data Extraction attempts to retransmit the report files based upon the settings of the following two installation parameters:

- “Number of Retry for Push Mode” (p. 6-120)
- “Retry Interval (Minutes) for Push Mode” (p. 6-121)

If all attempts fail, Data Extraction raises the “DET_PUSH_FAILED” (p. 42-11) platform alarm.

Errors can occur during the **ftp** process. The following errors are reported to both a trace file and the User Activity Log:

```
Directory xxxx not existed on remote server xxxx
```

This report error occurs when the DET.X_REMOTE_DIRECTORY parameter setting is empty or the named directory does not exist on the remote machine.

```
File creation error
```

This report error occurs when **ftp** fails because a file cannot be overwritten or the ftp session had to be terminated abnormally.

```
Login xxxx failed on remote server xxxx <(login)/(password)>
```

This report error occurs when the DET.X_REMOTE_LOGIN or DET.X_REMOTE-_PASSWORD parameter setting is empty or the password login failed on the remote machine.

```
Machine xxxx is not available
```

This report error occurs when the DET.X_REMOTE_MACHINE parameter setting is empty or the remote machine is unavailable.

Push Mode, Detectable Errors

The errors that are detected when a file is pushed, are placed in the User Activity Log and the Data Extraction Tool logfile.

- Remote Machine is unavailable
- Login on Remote Machine refused
- The Remote Directory is not present
- File creation error

Push Mode, Remote Filename

Files from multiple OMSs can be transferred to the system. The file name that is transferred does not include the directory name.

Push Mode, Data to transfer

A notification file is created when the data extraction file is transferred successfully. Data transfer is done in two ways:

- Push a requested data extraction file
- Push a notification file

Push Mode, Retries

OMS tries N times to transfer a file and if all attempts fail, Data Extraction raises the "DET_PUSH_FAILED" (p. 42-11) platform alarm.

Data Extraction related platform alarm

The following hot link provides additional information on a platform alarm that is related to Data Extraction: "DET_PUSH_FAILED" (p. 42-11).

Data File Concepts

Data file definition and types

Data files are tab-delimited (tab-separated), predefined flat files that Data Extraction tool generates in ASCII format.

The first row of each data file contains column headings for each field. Each row of the data file is a separate record. Individual fields within the record row are delimited by a tab character.

Data files can be generated for the following:

- "Equipment Data Files" (p. 16-8)
- "All Alarm Data Files" (p. 16-17)
- "Active Alarm Data Files" (p. 16-19)
- "NE Data Files" (p. 16-21)
- "Network Connections Data Files" (p. 16-25)
- "PM Data Files" (p. 16-23)
- "Link Connection Data Files" (p. 16-27) (for 1625 LambdaXtreme® Transport)
- "Data Export Types" (p. 16-24)
- "For Export Modes" (p. 16-25)

Data file filename extension and viewing

Users can view the data files from a standard web browser by entering the server name or its IP address as the URL:

http://<hostname>.<domain.com>/data_extraction

-or-

http://<IP address>/data_extraction

Users can save a particular file to their desktops via the browser **Save as** and then view the file as a report in spreadsheet format.

In general, the data files follow the Tab Separated Value format, which produces a **.tsv** file type that is given an **.xls** file extension. With a **.xls** extension, the file can be opened as a spreadsheet using any tool that is capable of viewing tab separated files (such as Microsoft® Excel or its equivalent). When the file is viewed as **.xls** format, it is then referred to as a *report file* or a *report*.

Data file location

Regardless if the feature is executed automatically or manually, Data Extraction generates specific data files in various subdirectories that are created for each data file:

/var/opt/lucent/data_extraction/<DataType>

Data file retention period

The system retention period for the data files is specified through the installation parameters. Note the following:

- With the exception of the 15-minute PM data file, the default retention period value for all data files is three days and reports can be retained from one to seven days.
- For the 15-minute PM data file, the default retention period is one day and reports can be retained from one to three days.
- For Active Alarm data, the keyword *ALL* can be specified from the command line to extract all active alarms.
- The management system automatically purges or overwrites files older than the specified retention period.

Data Extraction report time zone

Except for PM reports, all reports are generated based on the host time that was specified during installation of the system. Time stamps used in all PM reports are reported using the UTC time zone. For details, see the "Time Zone" (p. 6-88) installation parameter.

Equipment Data Files

Equipment data file contents

The equipment data file is a snapshot of the circuit pack inventory information at a given point in time. Each file includes all circuit packs and associated inventory data for each NE.

Installation parameters that control equipment data files

The following installation parameters enable the collection of equipment data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable Equipment Report in Push/Pull Mode" (p. 6-95)
- "Equipment Report Retention Period (Days)" (p. 6-95)
- "Remote Machine IP for Push Mode Equipment Report" (p. 6-96)
- "Remote Machine Login ID for Push Mode Equipment Report" (p. 6-96)
- "Remote Machine Password for Push Mode Equipment Report" (p. 6-97)
- "Remote Directory Name for Push Mode Equipment Report" (p. 6-97)

Equipment data file filename and location

The equipment data file is named the following:

Eqpt_<NE type>_<date>.xls

The following table provides a description of each report field in the equipment data file.

Where: NE* type is one of the following:	NE Name*
ADM16_1	WaveStar® ADM 16/1
ADMC	1643 ADM MultiService Mux (Compact Shelf)
ADMU	1663 Add Drop Multiplexer (ADMu)
AM	1643 Access Multiplexer (AM)
AMS	1643 Access Multiplexer Small (AMS)
AMU	1655 Access Multiplexer Universal (AMU)
DDM2000	DDM-2000 OC3 Multiplexer
DMX	1665 DMX Access Multiplexer
DMXEP	1665 Data Multiplexer Explore (DMXplore)
DMXET	1665 DMXtend Access Multiplexer
EON	1694 Enhanced Optical Networking (EON)
LU	1675 Lambda Unite MultiService Switch (MSS)
LX	1625 LambdaXtreme® Transport
STM64	WaveStar® TDM10G (STM-64)
WSM	1695 Wavelength Services Manager (WSM)
AMC	1645 Access Multiplexer Compact (AMC)
*Refer to the "Summary of supported NEs" (p. 1-5) to determine if a particular NE is supported in this release of the management system.	

The equipment data file is located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/eqpt_data

The format of the file is as follows:

Eqpt_<Type>_<YYYYMMDD>.xls

1675 Lambda Unite MultiService Switch (MSS) equipment data report fields

The following table provides a description of each report field in the equipment data file for 1675 Lambda Unite MultiService Switch (MSS). Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

1675 Lambda Unite MultiService Switch (MSS)	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Name	The name of the circuit pack.
Circuit Pack Qualifier	The qualifier of the circuit pack.
Apparatus Code	A 9-character code that is only applicable to TNA NEs.
Series Number	A 6-character number that is only applicable to TNA NEs.
CLEI Code	10-character Common Language Equipment Identification Code.
ECI code	6-character Equipment Catalog Item code that is only applicable to TNA NEs.
Serial Number	A 1 to 25 character number.
Holder Status	No record if empty.
Operational State	Informational and not traditionally needed for inventory.
VLAN Tagging Mode	Informational and not traditionally needed for inventory.
LOXC switch capacity	Values are 0 (zero), which is the default, or 15. Within one NE, only one LOXC can be set to 15.
LO tributary standard	Values are SDH, SONET, or UNDEFINED (loswcap=0), which is the default.

1625 LambdaXtreme® Transport equipment data file report fields

The following table provides a description of each report field in the equipment data file for 1625 LambdaXtreme® Transport. Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

1625 LambdaXtreme® Transport	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.

1625 LambdaXtreme® Transport	
Report Field	**Remarks**
Circuit Pack Type	The type of circuit pack.
Apparatus Code	A 9-character code
Series Number	A 6-character number
Serial Number	A 1 to 25 character alphanumeric string.
CLEI Code	10-character Common Language Equipment Identification Code.
ECI code	6-character Equipment Catalog Item code
Frequency	Single frequency for fixed frequency OT. Range of frequency or tuned frequency for tunable OT
Supplier ID	For OMON circuit packs only.
Component Version Number	For OMON circuit packs only.
Component FW Version Number	For OMON circuit packs only.
Component FW Active Version in FMM	For OMON circuit packs only.
Component Serial Number	For OMON circuit packs only.
Optical Component Type	For OMON circuit packs only.

Metropolis® and WaveStar® NEs equipment data file report fields

The following table provides a description of each report field in the equipment data file for the 1643 ADM MultiService Mux (Compact Shelf), 1663 Add Drop Multiplexer (ADMu), 1643 Access Multiplexer (AM), 1643 Access Multiplexer Small (AMS), 1645 Access Multiplexer Compact (AMC), 1655 Access Multiplexer Universal (AMU), and WaveStar® ADM 16/1 NEs. Refer to the "Summary of supported NEs" (p. 1-5) to determine if these NEs are supported in this release of the management system.

1643 ADM MultiService Mux (Compact Shelf) 1663 Add Drop Multiplexer (ADMu) 1643 Access Multiplexer (AM) 1643 Access Multiplexer Small (AMS) 1645 Access Multiplexer Compact (AMC) 1655 Access Multiplexer Universal (AMU) WaveStar® ADM 16/1	
Report Field	**Remarks**
NE name	The name of the network element.*

1643 ADM MultiService Mux (Compact Shelf) 1663 Add Drop Multiplexer (ADMu) 1643 Access Multiplexer (AM) 1643 Access Multiplexer Small (AMS) 1645 Access Multiplexer Compact (AMC) 1655 Access Multiplexer Universal (AMU) WaveStar® ADM 16/1	
Report Field	**Remarks**
Circuit Pack ID	The circuit pack identifier.*
Expected Item Code	The expected type of circuit pack.
Actual Item Code Type	The actual type of circuit pack.*
Interchangeability Marker	The interchangeability marker.*
Comcode	The comcode.*
Serial Number	A 1 to 25 character alphanumeric string.*
VLAN Tagging Mode	Informational and not traditionally needed for inventory.
Adapter item code	Reported only if the 1655 Access Multiplexer Universal (AMU) adapter card is legacy AM units is deployed.
Adapter version number	Reported only if the 1655 Access Multiplexer Universal (AMU) adapter card is legacy AM units is deployed.
Adapter serial number	Reported only if the 1655 Access Multiplexer Universal (AMU) adapter card is legacy AM units is deployed.
Adapter product code	Reported only if the 1655 Access Multiplexer Universal (AMU) adapter card is legacy AM units is deployed.
* Includes support for NTUs/SRUs.	

Metropolis® DMXs and DDM-2000 OC3 equipment data file report fields

The following table provides a description of each report field in the equipment data file for the DDM-2000 OC3 Multiplexer, 1665 DMX Access Multiplexer, 1665 Data Multiplexer Explore (DMXplore), and 1665 DMXtend Access Multiplexer NEs. Refer to the “Summary of supported NEs” (p. 1-5) to determine if these NEs are supported in this release of the management system.

DDM-2000 OC3 Multiplexer 1665 DMX Access Multiplexer 1665 Data Multiplexer Explore (DMXplore) 1665 DMXtend Access Multiplexer	
Report Field	**Remarks**
NE name	The name of the network element.

DDM-2000 OC3 Multiplexer 1665 DMX Access Multiplexer 1665 Data Multiplexer Explore (DMXplore) 1665 DMXtend Access Multiplexer	
Report Field	**Remarks**
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Name	The name of the circuit pack.
Apparatus Code	A 10-character code.
Series Number	A 6-character number.
CLEI Code	10-character Common Language Equipment Identification Code.
ECI code	6-character Equipment Catalog Item code.
Program ID Code	Identifies the version of the firmware on one or more socketed devices on the circuit pack for the DDM-2000 OC3 Multiplexer only.
Serial Number	A 12 character alphanumeric string.
Software Version	The version of running software.
VLAN Tagging Mode	Informational and not traditionally needed for inventory.

1694 Enhanced Optical Networking (EON) equipment data file report fields

The following table provides a description of each report field in the equipment data file for the 1694 Enhanced Optical Networking (EON). Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

1694 Enhanced Optical Networking (EON)	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Type	The type of circuit pack.
Apparatus Code	A 32-character code
Series Number	A 6-character number
Serial Number	A 1 to 12 character alphanumeric string
CLEI Code	10-character Common Language Equipment Identification Code
ECI code	6-character Equipment Catalog Item code

1694 Enhanced Optical Networking (EON)	
Report Field	**Remarks**
Software Version	The version of running software

1695 Wavelength Services Manager (WSM) equipment data file report fields

The following table provides a description of each report field in the equipment data file for the 1695 Wavelength Services Manager (WSM). Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

1695 Wavelength Services Manager (WSM)	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Type	The type of circuit pack.
Serial Number	A 1 to 12 character alphanumeric string.
Alarm Reporting State	Reports DISABLED or ENABLED.
Regeneration mode	Reports the regeneration mode to be disabled or enabled.
Model number	A string.
Software load	A string.
Pack port control mode	Reports the mode to be Normal or Override.
Boot ROM version	An alphanumeric string of up to 7 characters.
Hardware revision number	An alphanumeric string of up to 2 characters.
Manufacture date	A string in the format of 'YYWW'
CPLD version number	A string.
FPGA 1 version	A string.
FPGA 2 version	A string.
Wavelength	The wavelength of the circuit pack, if applicable.
CLEI Code	10-character Common Language Equipment Identification Code.
*ASE table status 1 to 21	For RAMAN packs only; 21 sets of report data available.
*Pump power (mWatts)	For RAMAN packs only; 21 different values; 21 sets of report data are available.

1695 Wavelength Services Manager (WSM)	
Report Field	**Remarks**
*ASE level	For RAMAN packs only, the noise level; 21 sets of report data are available.
*Current pump power level	For RAMAN packs only; 21 sets or report data are available.

***Example:**
`ASE Table Status 1`
`Pump Power,ASE level,Current Pump Power Level 1`
...
`ASE Table Status 21`
`Pump Power,ASE level,Current Pump Power Level 21`	

WaveStar® TDM10G (STM-64) equipment data report fields

The following table provides a description of each report field in the equipment data file for WaveStar® TDM10G (STM-64). Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

WaveStar® TDM10G (STM-64)	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Name	The name of the circuit pack.
Circuit Pack Qualifier	The qualifier of the circuit pack.
Apparatus Code	A 9-character code that is only applicable to TNA NEs.
Series Number	A 6-character number that is only applicable to TNA NEs.
CLEI Code	10-character Common Language Equipment Identification Code.
ECI code	6-character Equipment Catalog Item code that is only applicable to TNA NEs.
Serial Number	A 1 to 25 character number.
Holder Status	No record if empty.
Operational State	Informational and not traditionally needed for inventory.
Equipment Status	Informational and not traditionally needed for inventory.
Provisioned State	Informational and not traditionally needed for inventory.

WaveStar® TDM10G (STM-64)	
Report Field	**Remarks**
Procedural Status	Informational and not traditionally needed for inventory.
Flashdisk Equippage	Informational and not traditionally needed for inventory.
Flashdisk Acceptability	Informational and not traditionally needed for inventory.
Availability Status	Informational and not traditionally needed for inventory.

1671 Service Connect (SC) equipment data report fields

The following table provides a description of each report field in the equipment data file for 1671 Service Connect (SC). Refer to the "Summary of supported NEs" (p. 1-5) to determine if this NE is supported in this release of the management system.

1671 Service Connect (SC)	
Report Field	**Remarks**
NE name	The name of the network element.
Circuit Pack ID	The circuit pack identifier.
Circuit Pack Type	The type of the circuit pack.
Circuit Pack Qualifier	The qualifier of the circuit pack.
Part Number	A 6-character number that is only applicable to TNA NEs.
Series Number	A 6-character number that is only applicable to TNA NEs.
CLEI Code	10-character Common Language Equipment Identification Code.
ECI code	6-character Equipment Catalog Item code that is only applicable to TNA NEs.
Serial Number	A 1 to 25 character number.
Holder Status	No record if empty.
Application Software Name	The name of running software.
Application Software Version	The version of running software.
Firmware Name	The name of the running firmware.
Firmware Version	The version of the running firmware.
Model	A string.
Revision	A string.

All Alarm Data Files

All Alarm data file contents

The All Alarm data files contain all raised and cleared alarms that the management system has received in a specified time interval for all NE types. The time interval is specified in days, by providing intervals that are backward in time from the present time.

Dates and times for alarm data are based on the date and time that is logged on the management system, not the date and time that is reported by and/or on the NEs. All date and time related fields (for example, those fields for Raise Date and Time or Clear Date and Time) are stored in the management system database in the UTC timezone. When the report is generated, those date and time fields are converted to the timezone that is specified on the server.

When in PUSH mode, the management system sends the All Alarm data file from its alarm log without providing any filtering. The receiving server is responsible to filter the required data.

Installation parameters that control the All Alarm data files

The following installation parameters enable the collection of all alarm data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- “Enable All Alarm Report in Push/Pull Mode” (p. 6-98)
- “Active Alarm Report Retention Period (Days)” (p. 6-102)
- “Interval (Days) for All Alarm Report” (p. 6-99)
- “Remote Machine IP for Push Mode All Alarm Report” (p. 6-100)
- “Remote Machine Login ID for Push Mode All Alarm Report” (p. 6-100)
- “Remote Machine Password for Push Mode All Alarm Report” (p. 6-101)
- “Remote Directory Name for Push Mode All Alarm Report” (p. 6-101)

All Alarm data file filename and location

The All Alarm data files are named the following:

All_Alarms_<YYYYMMDD>.xls

The alarm data files are located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/alarm_data

All Alarm data file report fields

The following table provides a description of each report field in the alarm data file.

Report Field	Remarks
Alarm ID	The ID of the Alarm. It is displayed in the Alarm List and Alarm Log.
EMS Alarm ID	The ID of the Element Management System (Controller) Alarm. It is displayed in the Alarm List and Alarm Log.
NE Name	It is displayed the Alarm List and Alarm Log.
NA Name	The name of the Network Adapter for the managing NE It is displayed in the Alarm List and Alarm Log.
SA/NSA	The service affecting value provided by the NE It is displayed in the Alarm List and Alarm Log.
Alarm Severity	It is displayed in the Alarm List and Alarm Log.
Alarm Status	It is only displayed in the Alarm List
Source	It is displayed in the Alarm List and Alarm Log.
Alarm Group	It is only displayed in the Alarm List
Probable Cause	It is displayed in the Alarm List and Alarm Log.
Alarm Description	It is displayed in the Alarm List and Alarm Log.
Raise Date & Time	It is displayed in the Alarm List and Alarm Log.
Clear Date & Time	It is displayed in the Alarm List and Alarm Log.
Acknowledge Status	It is only displayed in the Alarm List.
Acknowledged By	Can be the same as *Raise Acknowledge User* in the Alarm Log when the delete option is the default.
Raise Acknowledge User*	Can be the same as *Acknowledge by* in the Alarm List when the delete option is the default.
Acknowledge Date & Time	Can be the same as *Raise Acknowledge Date & Time* in the Alarm Log when the delete option is the default .
Raise Acknowledge Date & Time	Can be the same as *Acknowledge Date & Time* in the Alarm List when the delete option is the default.

Active Alarm Data Files

Active Alarm data file contents

The Active Alarm data files contain all of the currently raised alarms that the management system has received for a specified interval. Each file includes all received alarm set messages that management system received in the specified interval.

The time interval is specified in days, by providing intervals that are backward in time from the present time. For active alarm data files, the keyword of *ALL* can be specified to denote all active alarms from the command line or the "Interval (Days) for Active Alarm Report" (p. 6-103) installation parameter can be set to 99999.

Dates and times for alarm data are based on the date and time that is logged on the management system, not the date and time that is reported by and/or on the NEs. All date and time related fields (for example, those fields for Raise Date and Time or Clear Date and Time) are stored in the management system database in the UTC timezone. When the report is generated, those date and time fields are converted to the timezone that is specified on the server.

Installation parameters that control the Active Alarm data files

The following installation parameters enable the collection of active alarm data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable Active Alarm Report in Push/Pull Mode" (p. 6-102)
- "Active Alarm Report Retention Period (Days)" (p. 6-102)
- "Interval (Days) for Active Alarm Report" (p. 6-103)
- "Remote Machine IP for Push Mode Active Alarm Report" (p. 6-103)
- "Remote Machine Login ID for Push Mode Active Alarm Report" (p. 6-104)
- "Remote Machine Password for Push Mode Active Alarm Report" (p. 6-104)
- "Remote Directory Name for Push Mode Active Alarm Report" (p. 6-105)

Active Alarm data file filename and location

The Active Alarm data files are named the following:

Active_Alarms_<YYYYMMDD>.xls

The Active Alarm data files are located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/alarm_data

Active Alarm data file report fields

The following table provides a description of each report field in the alarm data file.

Report Field	Remarks
Alarm ID	The ID of the Alarm. It is displayed in the Alarm List and Alarm Log.
EMS Alarm ID	The ID of the Element Management System (Controller) Alarm. It is displayed in the Alarm List and Alarm Log.
NE Name	It is displayed the Alarm List and Alarm Log.
NA Name	The name of the Network Adapter for the managing NE It is displayed in the Alarm List and Alarm Log.
SA/NSA	The service affecting value provided by the NE It is displayed in the Alarm List and Alarm Log.
Alarm Severity	It is displayed in the Alarm List and Alarm Log.
Alarm Status	It is only displayed in the Alarm List
Source	It is displayed in the Alarm List and Alarm Log.
Alarm Group	It is only displayed in the Alarm List
Probable Cause	It is displayed in the Alarm List and Alarm Log.
Alarm Description	It is displayed in the Alarm List and Alarm Log.
Raise Date & Time	It is displayed in the Alarm List and Alarm Log.
Clear Date & Time	It is displayed in the Alarm List and Alarm Log.
Acknowledge Status	It is only displayed in the Alarm List.
Acknowledged By	Can be the same as *Raise Acknowledge User* in the Alarm Log when the delete option is the default.
Acknowledge Date & Time	Can be the same as *Raise Acknowledge Date & Time* in the Alarm Log when the delete option is the default.

NE Data Files

NE data file contents

The NE data file is a snapshot of NE information at a given point in time. Each file includes all NEs of the management system and basic information identifying their type and software release.

Installation parameters that control the NE data files

The following installation parameters enable the collection of NE data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable NE Report in Push/Pull Mode" (p. 6-92)
- "NE Report Retention Period" (p. 6-92)
- "Remote Machine IP for Push Mode NE Report" (p. 6-93)
- "Remote Machine Login ID for Push Mode NE Report" (p. 6-93)
- "Remote Machine Password for Push Mode NE Report" (p. 6-94)
- "Remote Directory Name for Push Mode NE Report" (p. 6-94)

NE data file filename and location

The NE data file is named the following:

NE_<YYYYMMDD>.xls

It is located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/ne_data

NE data file report fields

The following table provides a description of each report field in the NE data file.

Report Field	Description
NE Name	Name/identifier of the NE
NE Type	Type/model of the NE
NE Version	NE release/software version

IP Data Files

IP data file contents

The IP data file is a snapshot of NE/IP/NSAP information at a given point in time. Each file includes all NEs of the management system.

Installation parameters that control the IP data files

The following installation parameters enable the collection of IP data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable NE Report in Push/Pull Mode" (p. 6-92)
- "NE Report Retention Period" (p. 6-92)
- "Remote Machine IP for Push Mode NE Report" (p. 6-93)
- "Remote Machine Login ID for Push Mode NE Report" (p. 6-93)
- "Remote Machine Password for Push Mode NE Report" (p. 6-94)
- "Remote Directory Name for Push Mode NE Report" (p. 6-94)

IP data file filename and location

The IP data file is named the following:

IP_<YYYYMMDD>.xls

It is located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/ne_data

IP data file report fields

The following table provides a description of each report field in the IP data file.

Report Field	Description
PRIGNE	Name of the primary GNE
TID	Name/identifier of the NE
IPADDR	IP Address of the NE
NSAP	NSAP address of the NE
SECGNE	Name of the secondary GNE

PM Data Files

PM data file contents

Data Extraction for PM data is supported for directly managed NEs only.

The PM data files includes all measured performance parameters and their values for the following:

- 24-hour PM data, in which users can specify an interval of 1 to N days of data, where N can be up to 30 days. The default interval is 3 days.
- 15-minute PM data, in which users can specify an interval of 1 to N hours of data, where N can be up to 72 hours. The default interval is 24 hours.

The data content of the PM files is supported by two formats:

- Legacy
- Current

Installation parameters that control the PM data files

The following installation parameters enable the collection of 15-minute and 24-hour data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable PM 15min Report in Push/Pull Mode" (p. 6-113) and "Enable PM 24HR Report in Push/Pull Mode" (p. 6-109)
- "PM 15min Report Retention Period (Days)" (p. 6-113) and "PM 24HR Report Retention Period (Days)" (p. 6-109)
- "Interval (Hours) for PM 15min Report" (p. 6-114) and "Interval (Days) for PM 24HR Report" (p. 6-110)
- "Remote Machine IP for Push Mode PM 15min Report" (p. 6-114) and "Remote Machine IP for Push Mode PM 24HR Report" (p. 6-110)
- "Remote Machine Login ID for Push Mode PM 15min Report" (p. 6-115) and "Remote Machine Login ID for Push Mode PM 24HR Report" (p. 6-111)
- "Remote Machine Password for Push Mode PM 15min Report" (p. 6-115) and "Remote Machine Password for Push Mode PM 24HR Report" (p. 6-111)
- "Remote Directory Name for Push Mode PM 15min Report" (p. 6-116) and "Remote Directory Name for Push Mode PM 24HR Report" (p. 6-112)

PM data file filenames and location

The PM DATA files are named the following:

BPM_15min_<YYYYMMDDHHmm>.xls for CMISE and TL1 NEs

BPM_24hr_<YYYYMMDDHHmm>.xls for CMISE and TL1 NEs

These files are located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/pm_data

Report format

For the default PM report format for both TP and Bulk modes, each row of the file consists of the following fields, with each field separated by a tab character:

- **NE Name**, which is the name of the network element.
- **Layer Rate**, which is the layer rate returned by the network element.
- **Granularity**, which is whether the data applies to the 15 minute or the 24 hour PM collection.
- **Port**, which is the AID of the port in the format generated by the network element.
- **First Bin**, which is the time of the first bin to which the data applies.
- **Last Bin**, which is the time of the last bin to which the data applies.
- **Counter Name**, which is the name of the counter.
- **Counter State**, which is one of the following single characters:
V indicates valid.
U indicates unavailable.
I indicates invalid.
- **Counter Value**, which is the numerical or other value of the counter.

For a detailed counter information, refer to the *OMS Service Assurance Guide*.

Data Export Types

Data Export type contents

Data Extraction for data export types is supported by two file formats.

- Legacy - This is applicable for CMISE NEs only. When the system is in TP Mode, the CMISE data is collected in Legacy format.
- Current - This is applicable for TL-1 NEs only. When the system is in TP Mode or Bulk Mode, the TL-1 data is collected in Current format.

For Export Modes

For Export mode contents

Certain export modes provide maximum backward compatibility by extracting only TL-1 PM data from BPM in the following format:

- Legacy - When the system is in TP mode.
- Current - When the system is in Bulk mode.

A system parameter **DET.LEGACY_EXTRACTION** enables certain export modes with values **ON** or **OFF**.

Network Connections Data Files

Network Connections data file contents

The Network Connections data file is a snapshot of network connections at a given point in time. Each file contains all network connections in the management system and some status information about these network connections.

Installation parameters that control Network Connections data files

The following installation parameters enable the collection of network connection data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- "Enable Network Connection Report in Push/Pull Mode" (p. 6-106)
- "Network Connection Report Retention Period (Days)" (p. 6-106)
- "Remote Machine IP for Push Mode Network Connection Report" (p. 6-107)
- "Remote Machine Login ID for Push Mode Network Connection Report" (p. 6-107)
- "Remote Machine Password for Push Mode Network Connection Report" (p. 6-108)
- "Remote Directory Name for Push Mode Network Connection Report" (p. 6-108)

Network Connections data file filename and location

The equipment data file is named the following:

Connection_<YYYYMMDD>.xls

It is located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/nc_data.

Network Connections data file report fields

The following table provides a description of each report field in the network connections data file.

Report Field	Description
Connection Name	The name of the network connection.
Connection Rate	The rate of the network connection.
Customer Name	The name of the customer.
Service Type	The service type of the network connection.
Protection Type	The protection type associated with the network connection.
Order Type	The order type associated with the network connection.
Order Number	The order number associated with the network connection.
Connection Alias	The connection alias associated with the network connection.
Order Step	The order step of the order.
Step State	The step state of the order.
Ignore Alarm for Completion	Regarding network connections, the alarm is ignored for completion to occur.
NE A1	The beginning NE in the network connection.
NE A2	The beginning NE in the network connection.
NE Z1	The ending NE in the network connection.
NE Z2	The ending NE in the network connection.
A1 Port ID	The beginning port of the network connection.
A2 Port ID	The beginning port of the network connection.
Z1 Port ID	The ending port of the network connection.
Z2 Port ID	The ending port of the network connection.
Routing Mode	The routing mode, which can be automatic, manual, or cross-connection based.
Shape	The shape of the network connection.
Implementation Date and Time	The date and time in which the network connection was put implemented/created.
In Effect Date and Time	The date and time in which the network connection was put into effect.

Link Connection Data Files

Link Connection data files contents

For 1625 LambdaXtreme® Transport, Data Extraction tool extracts and prepares field delimited files that summarize the capacity and usage information for each high speed DWDM physical network connection (for each Optical Multiplex Section) that the management system inventories.

Physical network connection information and the contained link connection information is listed. Each Optical Multiplex Section can have up to 64 double, simple uni-directional link connections (128 uni-directional link connections). Each bi-directional link connection in a physical network connection is represented by a unique sequence number that is reflected in the Data Extraction file.

Data Extraction reports the link connections only for a network connection that is in the *Implementation Complete* or *In-Effect* state.

Since the tool extracts link connection components that are unidirectional, the sequence number is repeated for each direction of a link connection.

Each line in the report can be a physical network connection name followed by the link connection that contains status information.

Installation parameters that control Link Connection data files

The following installation parameters enable the collection of link connection data, specify the retention period for the data, and specify machine particulars when in PUSH mode:

- “Enable Link Connection Report in Push/Pull Mode” (p. 6-116)
- “Link Connection Report Retention Period (Days)” (p. 6-117)
- “Remote Machine IP for Push Mode Link Connection Report” (p. 6-117)
- “Remote Machine Login ID for Push Mode Link Connection Report” (p. 6-118)
- “Remote Machine Password for Push Mode Link Connection Report” (p. 6-118)
- “Remote Directory Name for Push Mode Link Connection Report” (p. 6-119)

Link Connection data file filename and location

The link connection data file is named the following:

LX_OTS_LC_<YYYYMMDD>.xls

It is located in the following directory on the HP® server:

/var/opt/lucent/data_extraction/lc_data

Link Connection data file report fields

The following table provides a description of each report field in the link connections data file. The data is included when file type usage data and a specific date and time are specified. The data is displayed per port.

Report Field	Description
Connection Rate	The physical link (OCH).
Connection Name	The name of the physical link.
Number	A unique sequence number for the contained bidirectional LCs.
From NE	The source NE.
To NE	The sink NE.
From port	The source port.
To port	The destination port.
State	Available or Connected are the only link connection states that are applicable for 1625 LambdaXtreme® Transport cross connection-based connections.

Access Help for Data Extraction

When to use

Use this task to access the Data Extraction help screen from the command line.

Related information

See the following topic in this document:

- “Data Extraction Concepts” (p. 16-2)

Before you begin

Regardless of the setting of the “Enable/Disable DET Report Cron” (p. 6-120) installation parameter, Data Extraction can always be run manually and on-demand from the command line, providing the “OMS_DET license” (p. 5-6) is installed. To determine if the “OMS_DET license” (p. 5-6) is installed, see the “View a List of Licenses” (p. 5-17) task.

Task

Complete the following steps to access the Data Extraction help screen from the command line.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Execute the following command line:

```
DataExtraction -h
```

Result: The Data Extraction help screen is displayed.

END OF STEPS

Run Data Extraction Manually from the Command Line

When to use

Use this task to run Data Extraction manually and on-demand from the command line.

Related information

See the following topic in this document:

- "Data Extraction Concepts" (p. 16-2)

Before you begin

Regardless of the setting of the "Enable/Disable DET Report Cron" (p. 6-120) installation parameter, Data Extraction can always be run manually and on-demand from the command line, providing the "OMS_DET license" (p. 5-6) is installed. To determine if the "OMS_DET license" (p. 5-6) is installed, see the "View a List of Licenses" (p. 5-17) task.

The command to execute the report manually is as follows:

```
opt/lucent/platform/bin/DataExtraction [ ne_data | ip_data |
equipment | nc_data | lc_data | all_alarm days_to_collect |
active_alarm days_to_collect | pm24hr days_to_collect | pm15min
hours_to_collect | push]
```

Where: **ne_data** is network element type/release data

ip_data is network element IP and NSAP data

equipment is equipment data

nc_data is network connection data

lc_data is link connection data

all_alarm is all alarm data

active_alarm is active alarm data

pm15min is 15 minute PM data

pm24hr is 24 hour PM data

days_to_collect is a value that is equivalent to the current date/time, which determines the date/time to stop collection of data. The [days_to_collect] value also determines the date/time to start collection. For snapshot data (**ne_data** or **equip**), a **[days_to_collect]** value is not needed.

push allows you to manually transfer files to an existing remote machine

Task

Complete the following steps to run Data Extraction manually and on-demand from the command line.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Execute Data Extraction by entering the following command line:

```
DataExtraction [ ne_data | ip_data | equipment | nc_data | all_
alarm days_to_collect | active_alarm days_to_collect | pm24hr
days_to_collect | pm15min hours_to_collect | push]
```

Result: Data Extraction executes. Readily identifiable subdirectories for each report type are created. Data files are stored in the following directory:

/var/opt/lucent/data_extraction/<type>

The data files in each directory are named by the date and time of the report type (data file).

The log file is available if you follow this path:

/var/opt/lucent/logs/oms/tools/DataExtraction.log

END OF STEPS

17 Northbound Support

Overview

Purpose

This chapter explains the concepts and any needed tasks to administer northbound support.

Contents

Integrating Operations with External OSS Interfaces for Northbound Support

Northbound TL1 Alarm Interface

OMS provides a northbound Translation Language 1 (TL1) over TCP/IP interface for Operations Support Systems (OSSs) to receive autonomous TL1 alarm messages from the NEs.

OMS provides gateway and security functions for this interface by virtue of the following:

- The management system provides a *gateway function*. The OSS must support only a TCP/IP interface and have a single IP connection to OMS. The management system maintains TCP/IP connections to the NEs. The northbound system also benefits from the management system option of having redundant communications paths to the NEs.
- The management system enforces security over the interface. Northbound systems must use a login on the management system that invokes security screening. This login serves to authenticate the northbound system and to identify its privileges.

Refer to the "Retrieve Northbound TL1 Alarms" (p. 17-7) task.

Northbound TL1 Alarm Interface supported platforms

The Northbound TL1 Alarm Interfacel is supported on the *Server Platforms*. The Northbound TL1 Alarm Interface is not supported on the *PC Platform*.

Northbound TL1 Alarm interface as a licensable feature

The Northbound TL1 Alarm Interface is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the Northbound TL1 Alarm Interface requires the "OMS_TL1_ALARM license" (p. 5-15), which is typically installed during the initial installation of the management system. If the Northbound TL1 Alarm Interface license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

Northbound TL1 Alarm interface port assignment

The Northbound TL1 Alarm interface can be accessed remotely without logging in to the management system server. The port number (service number/socket) that is dedicated to the Northbound TL1 Alarm Interface is listed in the "Table of management system port assignments" (p. 40-1).

TMF814 CORBA™ Interface

A standard, licensed TMF814 CORBA™ interface

A standard Telemanagement Forum (TMF) 814 CORBA™ interface is supported that includes termination points, subnetwork connections, fault management, and performance management. This interface permits OMS to embed its operations environment with that of the service provider to enable flow-through operations with Alcatel-Lucent iOperations OSSs, third-party OSSs, and/or home-grown OSSs.

For additional details, see Chapter 18, “TMF814 Northbound Interface”.

MTOSI for Northbound XML Support

Northbound XML support

Multi-Technology Operations System Interface (MTOSI) is a licensed, northbound Extensible Markup Language (XML) interface from OMS to a service requestor that conforms to TMF854 Northbound Interface Standards for MTOSI. OMS functions as a service provider and other MTOSI clients, such as Alcatel-Lucent's Dynamic Network Analyzer (DNA), function as service requestors. The communication between the OMS MTOSI and its clients is accomplished via JMS; JBOSSMQ is used to transport the XML.

For additional details, see Chapter 19, “MTOSI”.

TIM Interface for a Northbound OSS

TIM definition

The TMN Integration Module (TIM) is an ASCII alarms interface that provides for the transfer of alarm data from the management system to a northbound interface (NBI), such as a northbound Operations Support System (OSS).

The management system server supports one OSS across the TIM interface.

TIM supported platforms

The use of the TIM interface is supported on the *Server Platforms*. The use of the TIM interface is also supported on the *PC Platform*.

TIM license

The TIM interface is an optional licensed feature that is only available to customers who have purchased and installed this feature. See Chapter 5, "Licensing" for details. The successful operation of the TIM interface requires the "OMS_TIM license" (p. 5-15), which is typically installed during the initial installation of the management system. If the TIM license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

TIM functionality

A TIM session is started when the upstream OSS has successfully logged into the management system. Typically, once a session is started, the cessation of a session by the OSS is considered an abnormal occurrence.

Once the OSS has logged in, currently active alarms in the management system are transferred to the OSS as part of the alarm synchronization process. Subsequent alarms are forwarded as they occur autonomously. The management system sends a heartbeat message to ensure that the periodic monitoring of the communications link is being performed.

TIM synchronization processing and forwarding alarms

All active persistent NE alarms, which are known to the management system at the time, are sent to the TIM interface during the synchronization process. After the synchronization process is completed, all NE alarms and management system platform alarms are forwarded autonomously through the TIM interface to the northbound OSS. Refer to "TIM Synchronous Data Transmission Terminology" (p. 6-141), "TIM Enable PSEs from Equipment Switch as Alarms" (p. 6-142), "TIM Enable PSEs from MSSPRING Switch as Alarms" (p. 6-142), "TIM Enable PSEs from RPR Switch as Alarms" (p. 6-143), "TIM Enable PSEs from TDM HO SNCP Switch as Alarms" (p. 6-143), "TIM Enable PSEs from TDM MSP Switch as Alarms" (p. 6-144), and "TIM Enable PSEs from WDM HO SNCP Switch as Alarms" (p. 6-144) installation parameters.

TIM alarm acknowledgement

The TIM interface does not provide a mechanism to acknowledge alarms remotely from the OSS. Auto-acknowledgement of forwarded alarms is not supported.

TIM interface security

Access to the management system over the TIM interface is protected by a login process, which relies on a user ID and password. The management system checks the user ID and password provided by the OSS with the values of the login and password installation parameters for compliance. The management system sends a login request response that confirms the login request is completed and a session is available or the login request is denied, at which point the session is automatically terminated by the management system server.

TIM installation parameters

Installation parameters for the TIM interface are initially set during the initial installation of the management system. These installation parameters control the filtering of service affecting (SA) and non-service affecting alarms (N-SA), the heartbeat interval of the interface, the user ID and password, and the timezone/timestamp. Refer to "TIM FM Filtering" (p. 6-140), "TIM Heartbeat Interval" (p. 6-140), "TIM Username" (p. 6-138), "TIM Password" (p. 6-139), and "TIM Timezone" (p. 6-139) installation parameters.

TIM port number assignment

Refer to "Table of management system port assignments" (p. 40-1) for the service/port number assigned to the TIM interface.

SNMP Interface

SNMP definition

SNMP is Simple Network Management Protocol, which is the network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices (routers, hubs, and switches), and to manage configurations, statistics collection, performance, and security.

SNMP Interface feature description

The management system provides an SNMP Interface to a northbound OS. Via installation parameters, the management system can be configured to transmit traps for alarms notifications to a port and IP address for the northbound OS. These traps are issued regardless of the northbound OS being present.

The northbound OS can request the management system to resend all active alarms that are logged on the system when it first starts up and then, dynamically, when it senses that alarms might have been missed due to network problems.

The northbound OS can request the management system to resynchronize alarms. During resynchronization, the management system forwards any currently raised persistent alarms to the northbound OS. Notifications of cleared alarms or transient alarms are not sent. While the resynchronization is in progress, the management system internally queues additional new alarms that have been raised and forwards them to the northbound OS at the end of the resynchronization.

SNMP Interface supported platforms

The use of the SNMP Interface is supported on the *Server Platforms*. The use of the SNMP Interface is not supported on the *PC Platform*.

SNMP Interface as a licensable feature

The SNMP Interface is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the SNMP Interface requires the "OMS_NB_SNMP license" (p. 5-10). If the SNMP Interface license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

For licensing restrictions imposed on the PC platform regarding the SNMP and TMF, refer to "OMS_NB_SNMP license" (p. 5-10).

SNMP Interface and related installation parameters

The operation of the SNMP Interface feature for northbound support is controlled by the following northbound installation parameters:

- "SNMP Address/Port Number" (p. 6-145)
- "SNMP Security Name" (p. 6-146)
- "SNMP Security Level" (p. 6-146)
- "SNMP Authentication Protocol" (p. 6-147)
- "SNMP Authentication Password" (p. 6-148)
- "SNMP Privacy Protocol" (p. 6-148)
- "SNMP Privacy Password" (p. 6-149)
- "SNMP Version" (p. 6-145)

SNMP Interface port assignment

Refer to "Table of management system port assignments" (p. 40-1) for the port that the management system will use for the SNMP Interface.

Retrieve Northbound TL1 Alarms

Purpose

Use this task to retrieve northbound TL1 alarms.

Related information

See the following topic in this document:

- "Northbound TL1 Alarm Interface" (p. 17-1)

Before you begin

You must know the OMS username and OMS password.

The port number (service number/socket) that is dedicated to the Northbound TL1 Alarm Interface is listed in the "Table of management system port assignments" (p. 40-1).

Task

Complete the following steps to retrieve northbound TL1 alarms.

1 At the prompt, **telnet** into the host server on which the management system is running:

```
telnet <hostname> <dedicated port number>
```

Example: `telnet ash 10160`

Recommendation: For HP® Serviceguard configurations, we recommend the use of the cluster IP or system logical name for the <hostname>.

Result: Output similar to the following should be displayed:

```
Trying...
Connected to <machine name>...
Escape character is '^]'
```

2 Enter the following activate user (ACT-USR) and correlation tag (CTAG) commands to activate you as the user on the host server.

```
ACT-USER:<host name>:<oms username>:CTAG::<oms password>;
```

Example: `ACT-USER:ash:oms_adm:akh::oms_adm+123;`

Result: Output similar to the following should be displayed:

```
<host name> <date> <time>
M <your login ID> COMPLD
```

Example:
```
ash 2004-07-01 11:38:51
   M akh COMPLD
```

3 Enter the following activate user (ACT-USR) and correlation tag (CTAG) commands to activate you as the user on the all NEs that the TL1 Northbound Alarms Interface is to manage:

```
ACT-USER:<NE name or TID>:<oms username>:CTAG::<oms password>;
```

Example: `ACT-USER:DMX1:oms_adm:akh::oms_adm+123;`

Result: Output similar to the following should be displayed:

```
<NE name or TID> <date> <time>
M <your login ID> COMPLD
```

Example:
```
DMX1 2004-07-01 11:38:53
   M akh COMPLD
```

All NE messages and alarms for the specified NE will be displayed in real time on the monitor where you are now logged in.

4 Enter the following cancel (CANC-USR) and correlation tag (CTAG) commands to de-activate you (log you out) as the user on the all NEs that the TL1 Northbound Alarms Interface is to manage:

```
CANC-USER:<NE name or TID>:<oms username>:CTAG;
```

Example: `CANC-USER:DMX1:oms:akh;`

5 Enter the following cancel (CANC-USR) and correlation tag (CTAG) commands to de-activate you (log you out) as the user on the host server:

```
CANC-USER:<host server>:<oms username>:CTAG;
```

Example: `CANC-USER:ash:oms:akh;`

END OF STEPS

18 TMF814 Northbound Interface

Overview

Purpose

This chapter provides conceptual and task information about the licensed Telemanagement Forum (TMF) 814 Northbound Interface.

Licensable feature

The TMF814 Northbound Interface is an optional licensable feature. It is only available to customers who have purchased and installed this feature.

Contents

TMF814 Northbound Interface Concepts

TMF814 Northbound Interface definition

The OMS TMF814 Northbound Interface (TMF814 NBI) is a standard, non-proprietary, machine-to-machine interface that enables a service provider operations support system (OSS) to have flow-through access to the provisioning, monitoring, and data collection capabilities of the OMS for the subnetwork(s) of NEs that it manages. The interface provides operational methods that allow any northbound service provider OSS to communicate with the management system and perform flow-through provisioning, alarm surveillance, and data collection on NEs, equipment, and connections within the management system domain, using Common Object Request Broker Architecture (CORBA™) object calls.

TMF814 Northbound Interface supported platforms

The use of the TMF814 Northbound Interface is supported on the *Server Platforms*. The use of the TMF814 Northbound Interface is not supported on the *PC Platform*.

TMF814 Northbound Interface as a licensable feature

The TMF814 Northbound Interface is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the TMF814 Northbound Interface requires the "OMS_TMF license" (p. 5-15) , which is typically installed during the initial installation of the management system. If the TMF814 Northbound Interface license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

For licensing restrictions imposed on the PC platform regarding the TMF and SNMP interfaces, refer to "OMS_TMF license" (p. 5-15).

TMF814 Northbound Interface support of the MTOSI feature

The TMF814 Northbound Interface supports the Multi-Technology Operations System Interface (MTOSI) through the management system interface. The MTOSI is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the MTOSI requires the "OMS_MTOSI license" (p. 5-9) and the "OMS_TMF license" (p. 5-15), which are typically installed during the initial installation of the management system. If the MTOSI and the TMF814 Northbound Interface licenses were not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

Refer to Chapter 19, "MTOSI" for more details on this feature.

TMF814 Northbound Interface naming services

Two external naming services can be registered. Refer to the "Naming Service" (p. 6-130) and installation parameters for details.

TMF814 Northbound Interface information model

The interactions between a service provider OSS and the OMS that are supported by the TMF814 Northbound Interface are governed by an information model that defines all objects, attributes, operations, and notifications used by the TMF814 Northbound Interface.

The information model for the interface consists of the following:

- The TMF814 CORBA™ IDL for each Management Functional Area (MFA) supported by the OMS
- The object and operational requirements defined in the *TeleManagement Forum Multi-Technology Network Management Business Agreement NML-EML Interface Version 2.1 (TMF 513)* and several methods from *Version 3.0*
- The CORBA™ objects, operations, and notifications defined in the *OMS - NML/EML Interface Behavior Document*

TMF814 Northbound Interface benefits

The design of the TMF814 Northbound Interface offers the service provider the following benefits:

- A uniform, multi-technology, protocol-independent information model that affords portability to Element Management Systems (EMSs) from different vendors without the need of customizing
- A modular set of programs that can be chosen and employed based on the service provider network management requirements
- Rapid service delivery by decreasing service activation time
- Faster introduction of new technologies in the network without requiring major changes to interfaces at the network management level
- Increased operating efficiency through automation and integration of network management and element management systems

TMF814 Northbound Interface basics

The OMS provides Element Management Layer support for one or more Network Communications Group (NCG)-connected subnetworks of NEs for a service provider OSS interacting through the TMF814 Northbound Interface and serves as the gateway to permit the Network Management Layer system to interact with NEs within its management domain.

Requests to provision or retrieve data from a network component managed by the OMS are sent by the service provider OSS through the TMF814 interface to the OMS. The OMS provisions the identified component or retrieves the requested data and sends notification of the change upstream to the service provider OSS through the TMF814 interface software.

Based on the type of provisioning or data request made, the service provider OSS issues a CORBA™ operational call through the interface software to get, set, create, operate, or delete an object instance and one or more object attributes. The object or object instance can be an NE or a hardware component within an NE. The object attributes can be a list of physical ports.

Notifications of any changes made to the transport network within the domain of the OMS are sent upstream to the service provider OSS through the TMF814 interface to keep the service provider OSS end-to-end view of the network synchronized with the portion of the network managed by the OMS.

A change made to a network component using the OMS or another interface (such as an NE CIT) can also trigger an autonomous event notification to the service provider OSS.

Network and platform system alarms and transient condition events are handled separately but in the same manner by the interface software. An alarm or event is received by the OMS, mapped to an equivalent CORBA™ alarm message by the TMF814 interface software, and forwarded upstream to the service provider OSS.

CORBA™ operational calls sent from the service provider OSS to the OMS and responses sent northbound from the OMS to the service provider OSS are all related to managed objects and object classes defined for the TMF814 Northbound Interface.

TMF814 Northbound Interface NE name mapping

The following table maps the name of the NE supported and the name by which the NE is known to the TMF814 Northbound Interface.

NE Name*	Known as by TMF814 NBI*
CBX-3500	CBX
DDM-2000 OC3 Multiplexer	DDM-OC3
1675 Lambda Unite MultiService Switch (MSS)	LUnite

NE Name*	Known as by TMF814 NBI*
1625 LambdaXtreme® Transport	Depending on the equipment: • LX_2F_ET • LX_2F_RPT_2 • LX_U_2D_ROADM • LX_U_1D_ROADM • LX_2D_ROADM • LX_MINILA • LX_3D_WXC • LX_4D_WXC • LX_3D_MINI_WXC (beyond R4.0) • LX_4D_MINI_WXC (beyond R4.0)
1643 ADM MultiService Mux (Compact Shelf)	ADM-C
1663 Add Drop Multiplexer (ADMu)	ADM-U
1643 Access Multiplexer (AM)	AM
1643 Access Multiplexer Small (AMS)	AMS
1655 Access Multiplexer Universal (AMU)	AMU
1665 DMX Access Multiplexer	DMX
1665 Data Multiplexer Explore (DMXplore)	DMXplore
1665 DMXtend Access Multiplexer	DMXtend
1694 Enhanced Optical Networking (EON)	EON
1695 Wavelength Services Manager (WSM)	Depending on the equipment: • WSM_OADM • WSM_ROADM • WSM_REPEATER
WaveStar® ADM 16/1	ADM_16/1
1645 Access Multiplexer Compact (AMC)	AMC
1671 Service Connect (SC)	1671 SC
* Refer to “Summary of supported NEs” (p. 1-5) for the appropriate NE releases that are supported.	

TMF814 Northbound Interface Configuration and Setup

TMF814 Northbound Interface software configuration

The TMF814 Northbound Interface runs on the standard server software as explained in "HP® Servers Software Platform" (p. 2-1) with the addition of the Iona Orbix® ASP Enterprise Edition Runtime software, Release 5.1. (Note: to change the Orbix® port number, refer to the "Change the Orbix® Port Number" (p. 40-9) task.)

The TMF814 Northbound Interface runs the standard PC-client software platform as explained in "Client hardware platform" (p. 2-3).

TMF814 Northbound Interface hardware configuration

The TMF814 Northbound Interface runs on the standard server hardware platform.

TMF814 Northbound Interface software installation

The TMF814 Northbound Interface software is installed with the management system on the same HP® client server. Once the OMS is installed, the TMF814 Northbound Interface is brought up automatically when the management system is brought up. Special procedures are not required. The standard startup and shutdown procedures for the management system also apply to the northbound interface software; refer to the "Start the Platform" (p. 9-5) and "Stop the Platform" (p. 9-7) tasks.

TMF814 Northbound Interface license

The successful operation of the TMF814 Northbound Interface requires the "OMS_TMF license" (p. 5-15). Feature licenses are typically installed, and thereby activated, upon the installation of the management system. Any subsequent additions of licenses are made with the "Add a License" (p. 5-18) task.

TMF814 Northbound Interface and Orbix® port numbers

The Orbix port number is set to default to port number 55075. This port number can be changed to a number from 55075 to 55079. To change the Orbix® port number, refer to the "Change the Orbix® Port Number" (p. 40-9) task.

TMF814 Northbound Interface installation parameters

The following installation parameters can be changed by a NOC administrator via a menu-driven interface program to ensure correct operation of the TMF814 Northbound Interface software or to optimize its performance:

- "Health Check Interval" (p. 6-129), and the recommended setting for the TMF814 Northbound Interface is 300 seconds.
- "Ping NMS Interval" (p. 6-129), and the recommended setting for the TMF814 Northbound Interface is 300 seconds.
- "Naming Service" (p. 6-130), and the recommended setting for the TMF814 Northbound Interface is naming service is LOCAL along with the "Secondary Naming Service" (p. 6-130), and the recommended setting for the TMF814 Northbound Interface is NONE, which is the default.
- "Connection Name Format" (p. 6-42), and the recommended setting for the TMF814 Northbound Interface has to be FREE, which is the default.
- "CTP Alarm Monitoring" (p. 6-46), and the recommended setting for the TMF814 Northbound Interface has to be ALL.
- "Orphan Cross Connection Deletion Tool" (p. 6-46), and the recommended setting for the TMF814 Northbound Interface has to be NO, which is the default.
- "Drop connections ending at CTP of SHDSL PTP" (p. 6-137), and the recommended setting for the TMF814 Northbound Interface has to be YES, which is the default.

The following installation parameters are also related to the TMF814 Northbound Interface:

- "MLSN Policy" (p. 6-131)
- "TMF SNC Naming" (p. 6-133)
- "TMF SNC End Point Rules" (p. 6-133)
- "TMF Unmanaged Domain Support" (p. 6-132)
- "TMF SNC Operation" (p. 6-132)
- "Drop connections ending at CTP of SHDSL PTP" (p. 6-137)

These installation parameters can be changed by following the procedures in the "Modify an Installation Parameter" (p. 6-167) task.

TMF814 Northbound Interface user preferences

The Date Format and Time Zone for the management system and its managed NEs must be set to ensure proper interaction with the service provider OSS user and the management system. The following fields must be set as shown for each service provider OSS user who accesses the management system:

- The **Date Format** field on the Preferences page must be set to the same date format used by the OSS. For instructions on how to view or set OMS user preferences, refer to the Set Preferences task in the *OMS Getting Started Guide*.
- The **Time Zone** setting for the OMS application, OMS server, and managed NEs must be the same.
  The time zone for the OMS application is set in the **Time Zone** field on the Preferences page.
  When an NE-to-OMS connection is added using the Add NE-OS Connection page, the time zone for the NE is set in the **NE time zone** field.
  For instructions on how to add a new NE-OS connection, refer to the Add an NE-OS Connection task in the *OMS Connection Management Guide*.

TMF814 Northbound Interface user role profiles

All management system users must have a user role profile that is associated with their management system account. Refer to "User Role Profile Concepts" (p. 7-2) for details.

In particular, the management system administrator and the person who is administering the TMF814 Northbound Interface must have the NOC Administrator factory-defined user role profile to perform many of the tasks associated with the interface; or, the management system administrator can also create another (copy) the NOC Administrator profile for the person who is administering the TMF814 Northbound Interface. See "NOC Administrator profile" (p. 7-3) for details.

Important! The NOC Administrator factory-defined user role profile should *never* be assigned to a service provider OSS user account (and user login) that is being used to access the OMS through the TMF814 Northbound Interface.

Management system users who are accessing the management system through the TMF814 Northbound Interface must have the factory-defined user role profiles of "NOC Expert Operator profile" (p. 7-3) or "NOC Operator profile" (p. 7-4).

Management system users who are accessing the management system through the TMF814 Northbound Interface and who need a user-defined user role profile, must have a user-defined user role profile that contains the "Connection Management user task" (p. 7-9).

TMF814 Northbound Interface User ID and password

Like all management system users, the service provider OSS users who must access the management system through TMF814 Northbound Interface must have a valid user account. Refer to "User Accounts Concepts" (p. 8-2), "User ID Rules" (p. 8-9), and "Password Rules" (p. 8-11) for details.

In addition, the service provider OSS users are subject to the same installation parameters that govern the session inactivity time outs and password use.

The user login inactivity timeout, which automatically times out a user after a specified period of time if inactivity on the management system occurs, does not apply to service provider OSS users who log into the OMS via the TMF northbound interface. However, this timeout does apply to management system users who login into the system directly; that is, through the management system *weblication*.

TMF814 Northbound Interface and character sets

To display or modify connections successfully, the character set that is used to specify a connection name from the TMF814 Northbound Interface should comply to the character set that is allowed from the OMS web interface. If the two character sets do not comply, any connections made from the TMF814 Northbound Interface on and/or from OMS web interface might not be displayed or modified properly.

Troubleshooting

Communication problems

If the service provider OSS cannot communicate with the OMS server, the IP address of the OMS server might not have been configured correctly in the **/etc/hosts** directory on the local service provider OSS server. To verify the IP address of the OMS server, follow the procedure described in the "Get the IP Address of the OMS Server" (p. 18-13) task.

The OMS application must be up and running for TMF814 Northbound Interface session with the service provider OSS to be working. Any problem that brings down the OMS application can cause an abrupt termination of the interface session.

If the interface session with the OMS is terminated gracefully or abruptly, the TMF814 Northbound Interface drops notifications destined for that session. The service provider OSS must re-establish the interface session.

Checking the interface connection

The client-server connection between the service provider OSS and the management system is periodically checked by the interface software by issuing a `ping` message. The frequency of the `ping` messages sent through the TMF814 Northbound Interface is controlled by a management system installation parameter; see the "Ping NMS Interval" (p. 6-129) section for details.

Health checks

Periodic health checks of the notification service, which provides object creation and change notifications from the management system to the service provider OSS, are made by issuing a health check notification message. A management system installation parameter controls the frequency of health check notification messages; see the "Health Check Interval" (p. 6-129) section for details.

Processing error recovery

If the management system detects an abnormal situation from which it cannot recover from gracefully, the management system terminates itself and the TMF814 Northbound Interface session, which causes the current OSS-to-management system interface session to be terminated.

If the management system detects an abnormal situation from which it can terminate gracefully, the management system automatically brings itself down, using the standard application shutdown procedure.

TMF814 Northbound Interface related platform alarms

The following hot links provide additional information on platform alarms that could be related to the malfunctioning of the TMF814 Northbound Interface:

- "NBI_SESSION_LOGOUT" (p. 42-20)

Set Up the TMF814 Northbound Interface for the NOC Administrator

When to use

Use this procedure to set up the TMF814 Northbound Interface for the NOC Administrator.

Related information

See the following topic in this document:

- "TMF814 Northbound Interface Configuration and Setup" (p. 18-6)

Before you begin

You must have a user account on the OMS that has the user role profile of NOC Administrator. In addition, you must have **`root`** login privileges on the machine on which the management system is running.

Task

Complete the following steps to set up the TMF814 Northbound Interface.

1 Bring up the management system using the standard startup procedure for the management system found in the "Start the Platform" (p. 9-5) task.

2 Log into the management system GUI. Determine if the "OMS_TMF license" (p. 5-15) was installed when the management system was initially installed using the "View a List of Licenses" (p. 5-17) task. If the license was installed, go to the next step.

If the OMS_TMF license was not installed, add the OMS_TMF license using the "Add a License" (p. 5-18) task.

3 If any installation parameters that are specific to the TMF814 Northbound Interface must be set to values other than their default installation settings, use the "Modify an Installation Parameter" (p. 6-167) task. Refer to "TMF814 Northbound Interface installation parameters" (p. 18-7) for a list of these parameters and additional links to details.

(**Note:** If you change the defaults for the "Naming Service" (p. 6-130) or the "Secondary Naming Service" (p. 6-130) installation parameters in this step, you must use the same names that you specified as new values for the installation parameters when editing the **/etc/hosts** file in the "Set Up Communication Between Servers" (p. 18-14) task.)

4 Set up communication between servers by completing the "Get the IP Address of the OMS Server" (p. 18-13) and "Set Up Communication Between Servers" (p. 18-14) tasks.

5 Determine the access needs for each service provider OSS user who must use the management system through the TMF814 Northbound Interface.

For those users who do not need customized user role profiles, assign the factory-defined user role profiles of NOC Expert Operator or NOC Operator using the "Copy a User Role Profile" (p. 7-24) task. For those users who need customized user role profiles, create a user-defined user role profile that includes the Connection Management task using the "Add a User-Defined User Role Profile" (p. 7-25) task. Note: for more details, see the "Connection Management user task" (p. 7-9).

6 Create a user account for each service provider OSS user who must use the management system through the TMF814 Northbound Interface using the "Add a User Account" (p. 8-15) task.

7 Inform all service provider OSS users who must use the management system through the TMF814 Northbound Interface that once they change their passwords on the management system, they can start to add NEs to the database to create a working view of the network within the management system domain. NEs are added in the standard method; refer all OSS users to the *OMS Network Element Management Guide* for details.

END OF STEPS

Get the IP Address of the OMS Server

When to use

Use this task to get the IP address of the OMS server.

Related information

See the following topic in this document:

- "Communication problems" (p. 18-9)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to get the address of the OMS server.

1 From the machine on which the management system is running, log in as **`root`**.

2 At the prompt, enter the following command:

```
grep <hostname> /etc/hosts
```

where **`<hostname>`** is the name of the OMS server.

Result: The IP address of the OMS **`<hostname>`** is displayed as the first field of the row in the **`/etc/hosts`** file.

END OF STEPS

Set Up Communication Between Servers

When to use

Use this task to set up communication between the NBI server and the management system HP® server.

Related information

See the following topics in this document:

- "Get the IP Address of the OMS Server" (p. 18-13)
- "Communication problems" (p. 18-9)

Before you begin

Before you begin to set up communication between the NBI server and the management system HP® server, determine the host name and the IP address of both the NBI and the management system HP® servers. Use the "Get the IP Address of the OMS Server" (p. 18-13) task to determine the IP address of the HP® server on which the management system is running.

Task

Complete the following steps to set up communication between the NBI server and the management system HP® server.

1 Enter the host name and IP address of the NBI server in the **/etc/hosts** file that resides on the management system HP® server. In addition, enter the external naming service and the IP address in the **/etc/hosts** file. (**Note:** If you changed the defaults for the Naming Service or the Secondary Naming Service installation parameters in Step 3 of the "Set Up the TMF814 Northbound Interface for the NOC Administrator" (p. 18-11) task, use the same names that you specified as new values for the installation parameters in the **/etc/hosts** file.)

2 Enter the host name and IP address of the management system HP® server in the **/etc/hosts** file that resides on the NBI server.

END OF STEPS

View Active TMF814 NBI Sessions

When to use

Use this procedure to view active TMF814 Northbound Interface (NBI) sessions.

Related information

See the following topics in this document:

- "TMF814 Northbound Interface Concepts" (p. 18-2)
- "TMF Session Administration user task" (p. 7-22)

Before you begin

You must have a user account on OMS that has the user role profile of NOC Administrator or any other profile that contains the "TMF Session Administration user task" (p. 7-22).

Task

Complete the following steps to view active TMF814 NBI sessions.

1 Use the icons or the object links to follow this path:

- **Management Network > OMS to OS TMF Communication**

  Result: The OMS to OS TMF Communication page is displayed.

2 Select **View TMF active sessions** and click **Search**.

Result: The table panel of the OMS to OS TMF Communication page is displayed, which lists the users names and times of login times. If active TMF sessions do not exist, the management systems informs you that

```
Currently there are no active TMF sessions.
```

END OF STEPS

Delete Active TMF814 NBI Sessions

When to use

Use this procedure to delete active TMF814 Northbound Interface (NBI) sessions.

Related information

See the following topics in this document:

- "TMF814 Northbound Interface Concepts" (p. 18-2)
- "View Active TMF814 NBI Sessions" (p. 18-15)
- "TMF Session Administration user task" (p. 7-22)

Before you begin

You must have a user account on the OMS that has the user role profile of NOC Administrator or any other profile that contains the "TMF Session Administration user task" (p. 7-22).

Requests to delete an active TMF814 NBI session automatically close any adjunct processes or purge any buffers.

Step 1 of this task requires you to complete the "View Active TMF814 NBI Sessions" (p. 18-15) task.

Task

Complete the following steps to delete active TMF814 NBI sessions.

1 Complete the steps in the "View Active TMF814 NBI Sessions" (p. 18-15) task.

2 Select the session or session to be deleted. In addition, select single or multiple users.

3 From the Go menu, select **Delete Session(s)** and click the **Go** button.

Result: The indicated user sessions are deleted. To view an updated page, go to Step 4 .

If the session cannot be deleted, the system responds with an appropriate message indicating that a particular user name deletion failed; check the user name and retry. To view what is currently listed, go to Step 4.

4 To view an updated page, click **Refresh**.

Result: The table on the OMS to TMF Communication page is updated accordingly.

END OF STEPS

View Active Iterators Sessions

When to use

Use this procedure to view active iterators.

Related information

See the following topic in this document:

- "TMF814 Northbound Interface Concepts" (p. 18-2)

Before you begin

You must have a user account on the OMS that has the user role profile of NOC Administrator or any other profile that contains the TMF Session Administration task.

Task

Complete the following steps to view active iterators.

1 Use the icons or the object links to follow this path:

- **Management Network > OMS to OS TMF Communication**

  Result: The OMS to OS TMF Communication page is displayed.

2 Select **View active iterators** and click **Search**.

Result: The table panel of the OMS to OS TMF Communication page is displayed, which lists the Iterator ID, the Iterator Name, and the User name. If active iterators do not exist, the management systems informs you of the following:

```
Currently there are no active Iterators.
```

END OF STEPS

Delete Active Iterators

When to use

Use this procedure to delete active iterators.

Related information

See the following topics in this document:

- "TMF814 Northbound Interface Concepts" (p. 18-2)
- "View Active Iterators Sessions" (p. 18-18)

Before you begin

You must have a user account on the OMS that has the user role profile of NOC Administrator or any other profile that contains the TMF Session Administration task.

Requests to delete an active iterator automatically close any adjunct processes or purge any buffers.

Step 1 of this task requires you to complete the "View Active Iterators Sessions" (p. 18-18) task.

Task

Complete the following steps to delete active iterators.

1 Complete the steps in the "View Active Iterators Sessions" (p. 18-18) task.

2 Select the iterator or iterators to be deleted.

3 From the Go menu, select **Delete Iterators(s)** and click the **Go** button.

Result: The indicated iterators are deleted. To view an updated page, go to Step 4.

If the iterator cannot be deleted, the system responds with an appropriate message indicating that a particular iterator ID could not be deleted; check the iterator list and retry. To view the current iterator list, go to Step 4.

4 To view an updated page, click **Refresh**.

Result: The table on the OMS to OS TMF Communication page is updated accordingly.

END OF STEPS

Activate the TMF814 Northbound Interface License

When to use

Use this procedure to activate the TMF814 Northbound license, “OMS_TMF license” (p. 5-15) after it has been installed using the “Add a License” (p. 5-18) task.

Related information

See the following topics in this document:

- “TMF814 Northbound Interface Concepts” (p. 18-2)
- “Add a License” (p. 5-18)
- “OMS_TMF license” (p. 5-15)

Before you begin

You need the **root** login (privileges) to complete this task.

Step 1 of this task requires you to complete the “Add a License” (p. 5-18) task.

Task

Complete the following steps to activate the “OMS_TMF license” (p. 5-15) after it has been installed.

1 Complete the steps in the “Add a License” (p. 5-18) task.

2 From the machine on which the management system is running, log in as **oms**.

Result: You are now logged in as **oms**.

3 Enter the following command to stop the management system application:

```
platform_cntrl stop
```

Result: The management system application is stopped.

4 From the machines on which the management system is running, log in as **root**.

Result: You are now logged in as **root**.

5 Enter the following command line to copy the appropriate old license.txt and license.txt.old information:

```
cp /etc/opt/iona/licenses.txt /etc/opt/iona/licenses.txt.old
```

6 Enter the following command line and option to set up Orbix for northbound communication:

```
/opt/lucent/platform/bin/ionarepair
```

Select option **a**.

7 From the machine on which the management system is running, log in as **oms**.

Result: You are now logged in as **oms**.

8 Enter the following command to start the management system application:

```
platform_cntrl start
```

Result: The management system application is started.

END OF STEPS

19 MTOSI

Overview

Purpose

This chapter provides conceptual and task information about the licensed Multi-Technology Operations System Interface (MTOSI).

Contents

MTOSI Concepts

MTOSI definition

Multi-Technology Operations System Interface (MTOSI) is a northbound Extensible Markup Language (XML) interface from OMS to a service requestor that conforms to TMF854 Northbound Interface Standards for MTOSI. OMS functions as a service provider and other MTOSI clients, such as Alcatel-Lucent's Dynamic Network Analyzer (DNA), function as service requestors. The communication between the OMS MTOSI and its clients is accomplished via JMS; JBOSSMQ is used to transport the XML.

MTOSI data retrieval

Data retrieval for MTOSI is accomplished via a request/response channel of JMS. Because OMS and the XML interface are both multi-threaded systems, concurrent requests are accepted. The configuration of OMS determines the maximum number of concurrent requests.

The functioning of MTOSI adheres to the following:

- The MTOSI client must ensure that each response queue is established on JMS before any communication can occur with them and OMS.
- OMS depends on the reliability of JMS to send a response to an MTOSI client.
- The MTOSI interface relies on the capabilities of the northbound TMF814 interface that OMS provides.
- The file transfer mechanism is supported through File Transfer Protocol (FTP) only. OMS has the FTP client; the MTOSI client must have an FTP server running to support the file transfer.

The following bulk data retrieval requests are supported for MTOSI clients:

- getInventory, which can be used to retrieve OMS inventory data
- getActiveAlarms, which can be used to retrieve all active alarms in bulk from OMS
- getHistoryPMData, which can be used to retrieve historical performance management (PM) data from OMS

MTOSI supported platforms

The Multi-Technology Operations System Interface (MTOSI) is supported on the *Server Platforms*. The Multi-Technology Operations System Interface (MTOSI) is not supported on the *PC Platform*.

MTOSI as a licensable feature

The Multi-Technology Operations System Interface (MTOSI) is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the MTOSI requires the “OMS_MTOSI license” (p. 5-9) and the “OMS_TMF license” (p. 5-15), which are typically installed during the initial installation of the management system. If the MTOSI and the TMF814 Northbound Interface licenses were not installed during the initial installation of the management system, see the “Add a License” (p. 5-18) task.

MTOSI-related installation parameters

The following installation parameters can be changed by a NOC administrator via a menu-driven interface program to ensure correct operation of the MTOSI:

- "MLSN Policy" (p. 6-131), and the recommended setting for the MTOSI is FULL_MESH.
- "TMF Unmanaged Domain Support" (p. 6-132), and the recommended setting for the MTOSI is DISABLED.
- "TMF SNC End Point Rules" (p. 6-133), and the recommended setting for the MTOSI is BBOX_NOT_ALLOWED.
- "TMF SNC Naming" (p. 6-133), and the recommended setting for the MTOSI is STANDARD.

These installation parameters can be changed by following the procedures in the "Modify an Installation Parameter" (p. 6-167) task.

Set Up Communication Between DNA and OMS

When to use

Use this procedure to set up communication between the Dynamic Network Analyzer (DNA) and OMS.

Related information

See the following topics in this document:

- "MTOSI Concepts" (p. 19-1)
- "Get the IP Address of the OMS Server" (p. 18-13)

Before you begin

You must have a user account on the OMS that has the user role profile of NOC Administrator. In addition, you must have **`root`** login privileges on the machine on which the management system is running.

Task

Complete the following steps to set up communication between DNA and OMS.

1 Bring up the management system using the standard startup procedure for the management system found in the "Start the Platform" (p. 9-5) task.

2 Log on to the management system GUI. Determine if the "OMS_MTOSI license" (p. 5-9) and the "OMS_TMF license" (p. 5-15) were installed when the management system was initially installed using the "View a List of Licenses" (p. 5-17) task. If the licenses were installed, go to the next step.

If the OMS_MTOSI and OMS_TMF licenses were not installed, add them using the "Add a License" (p. 5-18) task.

3 Complete the steps in the "View the Parameter Settings of an Installation Parameter" (p. 6-165) task to verify that the correct installation parameters for TMF814 and MTOSI are set.

If any installation parameters that are specific to the TMF814 Northbound Interface must be set to values other than their default installation settings, use the "Modify an Installation Parameter" (p. 6-167) task. Refer to "TMF814 Northbound Interface installation parameters" (p. 18-7) for a list of these parameters and additional links to details.

(**Note:** If you change the defaults for the "Naming Service" (p. 6-130) or the "Secondary Naming Service" (p. 6-130) installation parameters in this step, you must use the same names that you specified as new values for the installation parameters when editing the **/etc/hosts** file in the "Set Up Communication Between Servers" (p. 18-14) task.)

You can find the correct installation parameter settings for MTOSI in "MTOSI-related installation parameters" (p. 19-3).

4 Complete the steps in the "Get the IP Address of the OMS Server" (p. 18-13) task.

5 Enter the host name and IP address of the DNA server in the **/etc/hosts** file that resides on the management system HP® server. In addition, enter the external naming service and the IP address in the **/etc/hosts** file. (**Note:** If you changed the defaults for the Naming Service or the Secondary Naming Service installation parameters in Step 3 of the "Set Up the TMF814 Northbound Interface for the NOC Administrator" (p. 18-11) task, use the same names that you specified as new values for the installation parameters in the **/etc/hosts** file.)

6 Enter the host name and IP address of the management system HP® server in the **/etc/hosts** file that resides on the DNA server.

7 If a distributed BPM server is configured, run the `lt_add_controller` command on the OMS server to add the location of the BPM server. If the location of the BPM server is not added, PM history reports from the MTOSI interface will fail.

END OF STEPS

Prepare to Create a JMS Response Queue

When to use

Use this task to prepare to create a JMS response queue.

Related information

See the following topics in this document:

- "MTOSI Concepts" (p. 19-1)
- "View the Parameter Settings of an Installation Parameter" (p. 6-165)
- "MTOSI-related installation parameters" (p. 19-3)
- "Start the Platform" (p. 9-5)
- "Set Up Communication Between DNA and OMS" (p. 19-4)

Before you begin

You only have to create a response queue; the request queue has been made available for you.

For any changes that are made to the installation parameters and/or the **mtosi.properties** file to take effect, you must restart the management system platform. Refer to the "Start the Platform" (p. 9-5) task for details.

Task

Complete the following step to prepare to create a JMS response queue.

1 Complete the steps in the "View the Parameter Settings of an Installation Parameter" (p. 6-165) task to verify that the correct installation parameters are set on the server on which you are to execute the createOrDeleteJmsQueue script. You can find the correct installation parameter settings in "MTOSI-related installation parameters" (p. 19-3).

2 For inventory, performance monitoring (PM), and alarm requests only, additional steps must be completed for PM data collection.

Log in to the management system GUI and create a user account that has the following user ID and password:

user ID = **nbi1234**

password = **abc+1234**

Log out of the management system GUI.

From the machine on which the management system is running, log in as **`oms`**.

Change directories:

```
cd /opt/lucent/oms/config
```

Use **vi** or any text editor to access the **mtosi.properties** file. For example:

```
vi mtosi.properties
```

Scroll down the file until the following lines appear:

```
37  nbiUserName=nbi1234

38  nbiPassword=abc+1234
```

Verify that these lines contain the same user name and password as the account that you just created on the management system GUI. If, for some reason, the user name and password differ, change these lines to reflect a user name of **nbi1234** and a password of **abc+1234**.

Save any changes that you have made to the file. For example:

```
s*
```

3 For any changes that were to the installation parameters and/or the **mtosi.properties** file to take effect, complete the steps in the "Start the Platform" (p. 9-5) task to restart the management system platform.

4 Complete the steps in the "Create a JMS Response Queue" (p. 19-8) task.

END OF STEPS

Create a JMS Response Queue

When to use

Use this task to execute the createOrDeleteJmsQueue script to create a JMS response queue.

Related information

See the following topics in this document:

- "MTOSI Concepts" (p. 19-1)
- "Prepare to Create a JMS Response Queue" (p. 19-6)
- "Delete a JMS Response Queue" (p. 19-10)

Before you begin

You only have to create a response queue; the request queue has been made available for you.

Step 1 of this task requires you to complete the "Prepare to Create a JMS Response Queue" (p. 19-6) task.

Task

Complete the following step to execute the createOrDeleteJmsQueue script to create a JMS response queue.

1 Complete the steps in the "Prepare to Create a JMS Response Queue" (p. 19-6) task.

2 From the machine on which the management system is running, log in as **`oms`**.

3 Enter the following command line to change directories:

```
cd /opt/lucent/platform/bin
```

Result: You are now in the **bin** directory.

4 Enter the following command line to execute the script:

```
$./createOrDeleteJmsQueue
```

Result: The script begins to prompt you about information regarding the JMS queue that is to be created.

5 When the system prompts you `Want to [create|delete] JMS queue?`, enter **`create`**.

6 When the system prompts you `Enter Queuename to be created or quit to exit`, enter the name of JSM queue. For example: **`testJMSqueue`**.

Result: The file that you have specified is created. To verify that the file has been created, go to step Step 7.

7 Enter the following command to change directories to verify the existence of the file that you have just created:

```
cd /var/opt/lucent/jboss/oms/deploy/jms
```

Result: The file that you have created is displayed as:

```
<filename>-service.xml
```

For example:

```
testJMSqueue-service.xml
```

8 When the system prompts you `Enter Queuename to be create or quit to exit`, enter **`quit`**.

Result: You have now created a JMS queue and the script has exited.

END OF STEPS

Delete a JMS Response Queue

When to use

Use this task to execute the createOrDeleteJmsQueue script to delete a JMS response queue.

Related information

See the following topics in this document:

- "MTOSI Concepts" (p. 19-1)
- "Create a JMS Response Queue" (p. 19-8)

Before you begin

You only have to create a response queue; the request queue has been made available for you.

Task

Complete the following steps to execute the createOrDeleteJmsQueue script to delete a JMS response queue.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command line to change directories:

```
cd /opt/lucent/platform/bin
```

Result: You are now in the **bin** directory.

3 Enter the following command line to execute the script:

```
$./createOrDeleteJmsQueue
```

Result: The script begins to prompt you about information regarding the JMS queue that is to be created.

4 When the system prompts you `Want to [create|delete] JMS queue?`, enter **`delete`**.

5 When the system prompts you
`Enter Queuename to be deleted or quit to exit`, enter the name of JSM queue to be deleted. For example: **`testJMSqueue`**.

Result: The file that you have specified is deleted. To verify that the file has been deleted, go to step Step 6.

6 Enter the following command to change directories so you can verify the deletion of the file that you have just specified:

```
cd /var/opt/lucent/jboss/oms/deploy/jms
```

Result: The filename that you specified to be deleted is not displayed.

7 When the system prompts you
`Enter Queuename to be delete or quit to exit`, enter **`quit`**.

Result: You have now deleted a JMS queue and the script has exited.

END OF STEPS

20 Disaster Recovery

Overview

Purpose

This chapter explains the Disaster Recovery feature and the tasks needed to perform Disaster Recovery functions.

Licensable feature

Disaster Recovery is an optional licensable feature. It is only available to customers who have purchased and installed this feature.

Contents

Disaster Recovery Concepts

Probable causes of disaster

Disaster Recovery protects the OMS and its HP® server platform against hardware and software failures that could be caused by the following events:

- system failure, such as the failure of the system power supply or a system component
- site failure, such as a natural disaster or fire
- backplane failure
- processor failure
- any unplanned outage

The solution for Disaster Recovery

The OMS Disaster Recovery solution protects against the site system failure of an a diverse geographic standby (or secondary) system along with interconnecting networking. Each system acts as an integrated web and application server that provides full management system functionality. Via the setup of appropriate URLs, client terminals can access the HP® server that is running the management system.

Both the active and the standby systems are designed as *hardened configurations*, which include hot component redundancy of mirrored disks, dual processors, and backplanes. Both systems are equipped with duplicate HP® hardware, software (HP's operating system and the OMS software), software releases, and third-party software. In addition, both systems support data between each server.

The standby system exists in *warm standby* mode—it is shut down (not running). Data is replicated between the active and standby servers (and vice-versa based on conditions) at the disk volume block level using the VERITAS Volume Manager™ (data replication software) running over a TCP/IP network.

While in replication mode, the management system is enabled only at the site of the active system; the remote system is in standby mode, receiving data updates from the active system. Failover from the primary system to the secondary system is manual, with failover time estimated to be equivalent to the startup time of the OMS application. The system administrator manually starts the application/database, which in turn initiates communication to the managed NEs on the standby system if the active system fails.

In addition, administrators use command-line tools to initiate replication, to migrate the application from the primary system to the secondary system, to perform a failover from the secondary system, and to recover a failed system into standby mode.

Disaster Recovery supported platforms

Disaster Recover is supported on the *Server Platforms*. (Disaster Recovery requires additional software components on the HP® server platform.) Disaster Recover is not supported on the *PC Platform*.

Disaster Recovery licensing and required software

Disaster Recovery is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of Disaster Recovery requires the "OMS_DR license" (p. 5-7).

Important! If the Disaster Recovery license was not installed during the initial installation of the management system, a *scratch* installation is then needed.

For a list of the Veritas® software that is required for Disaster Recover, refer to "HP® server Disaster Recovery required software" (p. 2-3) for details.

In addition, refer to the "Enter a Veritas® License" (p. 20-26) task for instructions on how to re-install a Veritas® license.

Architecture for Disaster Recovery

Disaster Recovery for the management system consists of two identical HP® server systems, geographically separated, and their interconnections.

Each HP® server system houses three types of data. Each type of data is isolated onto separate disk groups on its respective system:

- Program (static) data
- Operational (dynamic) data
- Temporary (scratch) data

Each HP® server system has the following disk groups:

- *rootdg*, which includes the operating system, third-party software, along with application binaries, swap devices, and system *tmp* space
- *dbdg*, which includes all operational data, such as the Oracle® databases, dynamic flat files (NE backups, software), and the VERITAS Volume Replicator™ (VVR) storage replication log (SRL)
- *logdg*, which is the scratch disk area used for on-line database backups and logs

Each disk group consists of one or more physical disks and one or more data volumes. The VERITAS Volume Replicator™ is used to replicate all operational data (the *dbdg* disk group) between systems. Data in the *rootdg* and *logdg* disk groups is not replicated because this data is static or scratch. Replication is always unidirectional, from the active system to the standby system, though these roles can reverse from one system to the other due to a disaster or an operational necessity. All data within the *dbdg* disk group is inaccessible at the standby system while replication is operational.

Disaster Recovery and distributed web server architecture

The management system supports a distributed web server architecture. For Disaster Recovery configurations, each web server is associated with only one application server, which is either the primary or the standby. Because of this unique association, users must ensure that each web server is configured with the correct server hostname after failover. Note that the primary server neither knows nor cares about the locations of the web servers because the web server always initiates all communication.

Disaster Recovery related platform alarms

The following hot links provide additional information on platform alarms that are related to the malfunctioning of a Disaster Recovery configuration:

- "DR_ACTSECTOPRI" (p. 42-12)
- "DR_PRITOACTSEC" (p. 42-13)
- "DR_PRITOSEC" (p. 42-13)
- "DR_RESYNC_PAUSED" (p. 42-12)
- "DR_RESYNC_STARTED" (p. 42-12)
- "DR_RESYNC_STOPPED" (p. 42-13)
- "DR_RLK_CONNECT" (p. 42-14)
- "DR_SECTOPRI" (p. 42-13)
- "DR_SRL_OVERFLOW" (p. 42-14)
- "DR_SRL_WARN" (p. 42-14)

Disaster Recovery related tasks

The following hot links provide additional information on user tasks that are related to a Disaster Recovery configuration:

- "Check the Disaster Recovery Installation" (p. 20-6)
- "Initiate Replication" (p. 20-12)
- "Migrate the Role of the Active Server to the Standby Server" (p. 20-14)
- "Takeover the Active System" (p. 20-19)
- "Reinstate a System" (p. 20-22)
- "Resynchronize the Active System after an SRL Overflow" (p. 20-24)
- "Enter a Veritas® License" (p. 20-26)
- "Change Servers to a Simplex Configuration" (p. 20-28)

Time for Initial Replication

The duration of initial replication depends on the bandwidth of the network. For example, on a network with a 100Mb of bandwidth, command execution can take up to two hours to complete.

Bandwidth and Latency Specification

The recommended bandwidth and latency specifications for the link between Primary and Secondary Disaster Recovery is 10Mbit/s, latency <40ms (round trip), Uses UDP. The Disaster Recovery specification should allow a full initialization to be completed within 24 hours. A high specification (both higher bandwidth and lower latency) can be used to improve the initialization time. Initialization is required after any period in which the Disaster Recovery scheme is disabled.

Check the Disaster Recovery Installation

When to use

Use this task to check the disaster recovery installation before you begin any other disaster recovery-related task.

Related information

See the following topic in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "Configure a Secure Shell (SSH)" (p. 9-27) task

Before you begin

Bring the HP® server and the management system application down on both machines.

Step 19 of this task requires you to complete the steps in the "Configure a Secure Shell (SSH)" (p. 9-27) task.

Task

Complete the following steps to check the installation prior to beginning any disaster recovery task.

1 Verify that the CORE and management system installation has been completed by logging in as **root** and entering the following command:

```
swlist
```

Result: The system outputs a three column table that indicates the software that is installed. Installed on every system are the following products, whose names appear in the first column of the table: `Base-VXVM`, `BUNDLE11i`, `FEATURE11i`, `...`, `LT_BOOTSTRAP`, `ITorbixASP`, and `Oracle`.

2 Enter the following command to validate that the VERITAS® VxVM feature is installed and is licensed properly:

```
/sbin/vxlictest -n "VERITAS Volume Manager" -f VxVM
```

Result: The command outputs the following: `VxVM feature is licensed`.

3 Enter the following command to validate that the VERITAS® VVR feature is installed and is licensed properly:

```
/sbin/vxlictest -n "VERITAS Volume Manager" -f VVR
```

Result: The command outputs the following: `VVR feature is licensed`.

4 Enter the following command to validate that the correct number of disks are configured:

```
vxprint -d
```

Result: The command outputs a series of three tabular lists that contain the heading `Disk Group`. Go to the next step to verify the output.

5 Check the output of the **`vxprint`** command to determine if 2 disks are configured in **rootdg**, 4 disks are configured in **logdg**, and 12 disks are configured in **dbdg**.

6 Enter the following command lines to verify that the **dbdg_srl** logical volume was created.

```
vxprint –v | grep “^v” | grep dbdg_srl
```

Result: The following output is displayed:

```
v  dbdg_srl  dbdg_rvg ENABLED 32768000 SRL ACTIVE - -
```

or

```
v dbdg_srl fsgen ENABLED 32768000 - ACTIVE - -
```

7 On the management system server, enter the following command to verify that the appropriate number of file systems are mounted.

```
cat /etc/opt/lucent/platform/fstab | grep /osm/db/ | awk '{print
$2}'
```

Result: The command output resembles the following:

```
/osm/db/redo/current
/osm/db/redo/archived
/osm/db/db01
/osm/db/db04
/osm/db/db02
/osm/db/db05
/osm/db/db03
/osm/db/db06
```

8 If any one of the following are installed, go to Step 9:

CNA, TNA, NMA and BPM.

If none of the following are installed, go to Step 14:

CNA, TNA, NMA and BPM.

9 If CNA or TNA or NMA or BPM are installed, enter the following command line:

```
cat /etc/opt/lucent/platform/fstab | grep /cache/db/ | awk
'{print $2}'
```

Result: The command output resembles the following:

```
/cache/db/redo/current

/cache/db/db01

/cache/db/db02

/cache/db/db03
```

10 If TNA is installed, enter the following command line:

```
cat /etc/opt/lucent/platform/fstab | grep /tna/db/ | awk '{print
$2}'
```

If TNA is not installed, go to Step 11.

Result: The command output resembles the following:

```
/tna/db/db04

/tna/db/db05
```

11 If NMA is installed, enter the following command line:

```
cat /etc/opt/lucent/platform/fstab | grep /nma/db/ | awk '{print
$2}'
```

If NMA is not installed, go to Step 12.

Result: The command output resembles the following:

```
/nma/db/db04

/nma/db/db05
```

12 If CNA is installed, enter the following command line:

```
cat /etc/opt/lucent/platform/fstab | grep /cna/db/ | awk '{print
$2}'
```

If CNA is not installed, go to Step 13.

Result: The command output resembles the following:

```
/cna/db/db05
/cna/db/db04
```

13 If BPM is installed, enter the following command line:

```
cat /etc/opt/lucent/platform/fstab | grep /bpm/db/ | awk '{print $2}'
```

If BPM is not installed, go to Step 14.

Result: The command output resembles the following:

```
/bpm/db/db05
/bpm/db/db08
/bpm/db/db06
/bpm/db/db07
/bpm/db/db04
/bpm/db/db09
```

14 Verify that the contents of the **/etc/opt/lucent/platform/sys_config** files on both the primary and the secondary servers have the following installation parameters specified:

On the primary server:

```
system_install_type=duplex
system_logical_name=<name chosen during installation>
system_role=primary
remote_system_name=<secondary server name>
```

On the secondary server:

```
system_install_type=duplex
system_logical_name=<name chosen during installation>
system_role=secondary
remote_system_name=<primary server name>
```

Note: Make sure that the **system_logical_name** is identical on both servers.

15 Verify that the contents of the **/etc/opt/lucent/platform/sys_status** file on the primary and the secondary servers has the following installation parameter specified:

```
system_status=shutdown
```

16 Verify that the **/etc/hosts** file on both servers contains entries for the primary and the secondary servers.

17 Verify that **ssh** works between the primary and secondary servers without a password challenge.

On the primary server, input the following command:

```
ssh <secondary server name>
```

Result: If you logged in to the primary server without a password challenge, go to Step 18.

If a password challenge is displayed, some type of **ssh** setup is required. If local security permits .shosts-based authentication between systems, go to Step 19.

If .shosts authentication is not permitted, obtain help from local security administrators to set up certificate-based authentication between the primary and secondary servers.

18 Verify that **ssh** works between the secondary and primary servers without a password challenge.

On the secondary server, input the following command:

```
ssh <primary server name>
```

Result: If you are logged in to the primary server without a password challenge, go to Step 21.

19 Complete the steps in the "Configure a Secure Shell (SSH)" (p. 9-27) task.

20 Once .shosts-based authentication between systems is established, repeat Step 17 and Step 18, which are the steps for **ssh** verification.

Important! Do not go on to Step 21 until **ssh** works in both directions without password challenges.

21 Enter the following command on each processor to verify that the primary and secondary servers are in shut down mode:

```
su - oms -c "platform_cntrl status"
```

Result: The command output is similar to the following:

```
Overall System status...[shutdown]
platform...[Down]
oms...[Down]
tna...[Down]
```

22 Enter the following command to verify that replication is not running:

```
vradmin printrvg
```

Result: The command does not display any output.

END OF STEPS

Initiate Replication

When to use

Use this task to initiate replication.

Related information

See the following topics in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "Check the Disaster Recovery Installation" (p. 20-6)

Before you begin

Step 1 requires you to complete the "Check the Disaster Recovery Installation" (p. 20-6) task.

Task

Complete the following steps to initiate replication.

1 Complete all of the steps in the "Check the Disaster Recovery Installation" (p. 20-6) task.

2 Log in to the primary server as **root**.

3 Enter the following command to initiate replication:

```
/opt/lucent/platform/bin/rep_initialise dbdg
```

Result: Command execution proceeds and the duration of its completion depends on the bandwidth of the network. For example, on a network with a 100Mb of bandwidth, command execution can take up to two hours to complete.

While command execution is proceeding, monitor the initiate replication process with the command in the next step.

4 Enter the following command to monitor the status of the replication process that was begun in the previous step:

```
vxrlink -g dbdg -i300 status rlk_<StandbyServer>_dbdg_rvg
```

Result: The command outputs status every five minutes until completion, at which time, the command outputs the message: `...is up to date`. Go to the next step.

5 Once the replication status is `up to date`, on the primary and secondary servers, enter the following command to start the replication notify daemon the primary and secondary servers:

```
/opt/lucent/platform/bin/rep_monitor_rc start
```

6 On the primary and secondary servers, enter the following command to verify that the application running on the servers is still shut down:

```
su - oms -c "platform_cntrl status"
```

Result: The command output is similar to the following:

```
Overall System status...[shutdown]

platform...[Down]

oms...[Down]

tna...[Down]
```

7 On the primary server, log in as **`oms`**.

8 Enter the following command to start the application and the GUI web server:

```
platform_cntrl start
```

Result: The application and the GUI web server are started.

END OF STEPS

Migrate the Role of the Active Server to the Standby Server

When to use

Use this task to migrate the role of the active server to the standby server.

Related information

See the following topics in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "Check the Disaster Recovery Installation" (p. 20-6)
- "Configure a Secure Shell (SSH)" (p. 9-27) task

Before you begin

Migration can be performed on the active or standby system. Migration fails if communication between systems is not established or if the state of replication is unhealthy.

Step 3 of this task requires you to complete the steps in the "Configure a Secure Shell (SSH)" (p. 9-27) task.

Task

Complete the following steps to migrate the role of the active server to the standby server.

1 On the active server, log in as **`root`**.

2 Enter the following command to display application status information:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the application status on both servers, the following message must be displayed under the `Local` heading: `system_status=running` and the following status message must be displayed under the `Remote` heading: `system_status=shutdown`.

3 Verify that **ssh** works between the primary and secondary servers without a password challenge.

On the primary server, input the following command:

```
ssh <secondary server name>
```

Result: If you logged in to the primary server without a password challenge, go to Step 4.

If a password challenge is displayed, some type of **ssh** setup is required. If local security permits .shosts-based authentication between systems, go to "Configure a Secure Shell (SSH)" (p. 9-27).

If .shosts authentication is not permitted, obtain help from local security administrators to set up certificate-based authentication between the primary and secondary servers.

4 Verify that **ssh** works between the secondary and primary servers without a password challenge.

On the secondary server, input the following command:

```
ssh <primary server name>
```

Result: If you are logged in to the primary server without a password challenge, go to Step 6.

5 Once .shosts-based authentication between systems is established, repeat Step 3 and Step 4, which are the steps for **ssh** verification.

Important! Do not go on to Step 6 until **ssh** works in both directions without password challenges.

6 Enter the following command to verify that the status of the replication link (RLINK) is current:

```
vxrlink -g dbdg status rlk_<StandbyServer>_dbdg_rvg
```

Result: The status of the replication is current when the command outputs the message: `...is up to date`.

7 Enter the following command to go to the **oms** login:

```
su - oms
```

8 Enter the following command to stop the application and the GUI web server:

```
platform_cntrl stop
```

Result: The application and the GUI web server are stopped.

9 Enter the following command to exit back to the root login:

```
exit
```

10 Enter the following command to display application status information:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the application status on the two servers, the following message must be displayed under the `Local` heading: `system_status=shutdown` and the following status message must be displayed under the `Remote` heading: `system_status=shutdown`.

11 Enter the following command to begin migration:

```
/opt/lucent/platform/bin/rep_migrate_active dbdg <StandbyServer>
```

Result: You are asked if you want to continue with the migration.

12 Enter **y** for yes.

Result: The command line prompt is displayed.

13 On the standby server, log in as **root**.

14 Enter the following command to determine if the replication role of the standby server is active:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the replication role of the standby server, the following message must be displayed under the `Local` heading: `rep_role=active` and the following status message must be displayed under the `Remote` heading: : `rep_role=standby`.

Note: If the replication role is not active on the standby server, contact Alcatel-Lucent Customer Support Services for support. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

15 Enter the following command to reset the database:

```
/opt/lucent/platform/bin/rep_db_reset
```

16 Answer **y** or **n** when the system prompts you:

```
Do you want to use NE(s) in the NA database? (y/n).
```

Enter **y** and press the **Enter** key to get a superset of the NE list from the OMS and NA databases.

Enter **n** and press the **Enter** key to get an NE list based upon the OMS databases only.

Press the **Enter** key to take the default, which varies according to the system configuration.

Result: Depending on what you have selected, a message similar to the following is displayed:

```
NE List Sync will be <SUPERSET> based, press [ENTER] to
continue.
```

17 Press **Enter**.

Result: Key entries in the database are renamed from the old system name to the new system name—the database hostname and IP entries are modified and the CMISE (CNA), TL1 (TNA) and NMA databases are dropped and recreated. Note: the log file is located in **/tmp/rep_db_reset.log**. Once you receive the message `rep_db_reset successfully completed`, go to the next step.

18 Enter the following command to display application status information:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the application status on both servers, the following message must be displayed under the `Local` heading: `system_status=shutdown` and the following status message must be displayed under the `Remote` heading: `system_status=shutdown`.

19 If any distributed configurations (such as NA, GWS, SNMS, SC) are associated with this server, enter the following command to add the appropriate information:

```
/opt/lucent/platform/bin/lt_add_controller
```

20 Enter the following command to start the application:

```
su - oms -c "platform_cntrl start"
```

Result: The application is started.

21 Enter the following command to determine if the application is running:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate that the application is running, following message must be displayed under the `Local` heading: `system_status=running`.

22 Initiate a database synchronization for each NE once the NE communication state is up and the `sync needed status` is `YES`.

Note: to determine the type of "sync needed" status, log into the management system and navigate to the Database Synchronizations page using the following path: **Tools > Database Synchronizations**. Click **All NEs in the network** and in the Sync Needed column, look for **Yes.**

END OF STEPS

Takeover the Active System

When to use

Use this task to enable the standby system to acquire the right to run the application due to failed active system.

Related information

See the following topics in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "Check the Disaster Recovery Installation" (p. 20-6)

Before you begin

The current state for the application on the local system should remain shutdown.

Takeover can be performed at the standby system only. Takeover fails if the replication link between systems is still healthy—a migration should be performed in this case. Takeover also fails if replication has left the file systems in an unrecoverable state.

Task

Complete the following steps to enable the standby system to acquire the right to run the application from a failed active system.

1 Log in to the standby system as **`root`**.

2 Enter the following command to display application status information:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate that the two servers cannot communicate the following status message must be displayed under the `Local` heading: `rep_status=fail`.

3 Enter the following command to initiate the takeover:

```
/opt/lucent/platform/bin/rep_takeover_active dbdg
```

4 To validate that the standby server is now the active replication server, enter the following command:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the replication role of the standby server, the following status message must be displayed under the `Local` heading: `rep_role=active`.

5 Enter the following command to reset the database:

```
/opt/lucent/platform/bin/rep_db_reset
```

Result: Key entries in the database are renamed from the old system name to the new system name—the database hostname and IP entries are modified and the CMISE (CNA), TL1 (TNA) and NMA databases are dropped and recreated. Note: the log file is located in **/tmp/rep_db_reset.log**. Once you receive the message `rep_db_reset successfully completed`, go to the next step.

6 Answer **y** or **n** when the system prompts you:

```
Do you want to use NE(s) in the NA database? (y/n).
```

Enter **y** and press the **Enter** key to get a superset of the NE list from the OMS and NA databases.

Enter **n** and press the **Enter** key to get an NE list based upon the OMS databases only.

Press the **Enter** key to take the default, which varies according to the system configuration.

Result: Depending on what you have selected, a message similar to the following is displayed:

```
NE List Sync will be <SUPERSET> based, press [ENTER] to
continue.
```

7 Press **Enter**.

8 Enter the following command to display application status information:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate the application status on the standby server, the following message must be displayed under the `Local` heading: `system_status=shutdown`.

9 If any distributed configurations (such as NA, GWS, SNMS, SC) are associated with this server, enter the following command to add the appropriate information:

```
/opt/lucent/platform/bin/lt_add_controller
```

10 Enter the following command to start the application:

```
su - oms -c "platform_cntrl start"
```

Result: The application is started.

11 Enter the following command to determine if the application is running:

```
/opt/lucent/platform/bin/get_system_info
```

Result: The system outputs status information. To validate that the application is running, following message must be displayed under the `Local` heading: `system_status=running`.

12 Initiate a database synchronization for each NE once the NE communication state is up and the `sync needed status` is `YES`.

Note: to determine the type of “sync needed” status, log into the management system and navigate to the Database Synchronizations page using the following path: **Tools > Database Synchronizations**. Click **All NEs in the network** and in the Sync Needed column, look for **Yes.**

END OF STEPS

Reinstate a System

When to use

Use this task to reinstate a system—meaning, to enable the former, failed, active system to rejoin the Disaster Recovery setup as the new standby system.

Related information

See the following topic in this document:

- "Disaster Recovery Concepts" (p. 20-2)

Before you begin

The current state of the application on the failed server should remain shutdown. Reinstatement can be performed on the new active system only—view this as a *push* from the new active to the new standby, not a *pull*.

Task

Complete the following steps to reinstate a system.

1 Verify that the failed server has been repaired and is back on-line.

2 To reinstate the server with the currently active server, log in to the active server as **`root`**.

3 Enter the following command to initiate the reinstate process:

```
/opt/lucent/platform/bin/rep_reinstate_standby dbdg
```

Result: Command execution proceeds and the duration of its completion depends on the bandwidth of the network.

While command execution is proceeding, use the command in the next step to monitor the reinstate process.

4 Enter the following command to monitor the reinstate process that was initiated in the previous step:

```
vxrlink -g dbdg -i300 status rlk_<StandbyServer>_dbdg_rvg
```

Result: The command outputs status every five minutes until completion, at which time, the command outputs the following message: `...is up to date`.

5 Once the reinstate process is completed, enter the following command to verify the status of the application and replication on both servers:

```
/opt/lucent/platform/bin/get_system_info
```

Result: To validate the application and replication status on the two servers, the following sets of status messages must be displayed. Under the `Local` heading, the messages `system_status=running` , `rep_status=okay`, and `rep_role=active` must be displayed and under the `Remote` heading the messages `system_status=shutdown`, `rep_status=okay`, and `rep_role=standby` must be displayed. The system has now been reinstated.

END OF STEPS

Resynchronize the Active System after an SRL Overflow

When to use

Use this task to resynchronize the active system after the Storage Replicator Log (SRL) has overflowed; that is, after the "DR_SRL_OVERFLOW" (p. 42-14) platform alarm is raised.

Related information

See the following topic in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "DR_SRL_OVERFLOW" (p. 42-14) platform alarm

Before you begin

If the Replication link (RLINK) has been restored, the command used in this task replays the Data Change Map (DCM) log, clears the SRL overflow alarm, and continues to push all the data in the SRL to the standby server.

Task

Complete the following steps to resynchronize the active system after SRL overflow.

1 Log in to the active server as **`root`**.

2 Enter the following command to verify that the replication link is restored and healthy:

```
/opt/lucent/platform/bin/rep_healthcheck
```

3 Enter the following command to initiate the resynchronization process:

```
/opt/lucent/platform/bin/rep_resync dbdg
```

Result: The command replays DCM logs and the "DR_SRL_OVERFLOW" (p. 42-14) alarm is cleared.

4 Enter the following command to monitor the resynchronization process that was initiated in the previous step:

```
vxrlink -g dbdg -i300 status rlk_<StandbyServer>_dbdg_rvg
```

Result: The command outputs status every five minutes until completion, at which time, the command outputs the following message: `...is up to date`.

END OF STEPS

Enter a Veritas® License

When to use

Use this task to enter a Veritas® license.

Related information

See the following topics in this document:

- "Disaster Recovery Concepts" (p. 20-2)
- "HP® server Disaster Recovery required software" (p. 2-3)

Before you begin

The two types of Veritas licenses that might be required for any particular application are the following:

- Veritas® Volume Manager™, which provides disk mirroring and other functions that are needed for data replication, is required by OMS Standalone with Disk Mirroring and the OMS Disaster Recovery solution.
- Veritas® Volume Replicator™, which provides continuous data replication for remote recover sites, is required by the OMS Disaster Recovery solution.

Pay particular attention to the notes that are imbedded within the steps of this procedure. They offer important typing tips!

Task

Complete the following steps to enter a Veritas® license.

1 Log in to the active server as **`root`**.

2 Enter the following command to change directories:

```
cd /opt/lucent/install/bin
```

Result: The directory is changed to bin.

3 Enter the following command line to get to the license function:

```
. ./lt_license_funcs
```

Note that the string that you must type is the following:

dot space dot slash lt_license_funcs

4 To install the Veritas® Volume Manager™ license, go to Step 5.

To install the Veritas® Volume Replication™ license, go to Step 8.

5 To install the Veritas® Volume Manager™ license, enter the following command line:

```
install_vxvm_licence
```

Note that the string that you must type is *licence* and not *license*.

6 At the prompt `Do you want to install full vxvm/disk mirror ? (y|n|q):`, enter **`y`** and press **`Enter`**.

7 At the prompt `Please enter licence key for full vxvm/disk mirror:`, enter the license string and press **`Enter`**.

8 To install the Veritas® Volume Replication™ license, enter the following command line:

```
install_vvr_licence
```

Note that the string that you must type is *licence* and not *license*.

9 At the prompt `Do you want to install disk replication ? (y|q):`, enter **`y`** and press **`Enter`**.

10 At the prompt `Please enter licence key for disk replication:`, enter the license string and press **`Enter`**.

11 To verify that the Veritas licenses are installed, enter the following command:

```
vxlicrep
```

Result: The names of the installed licenses are displayed.

END OF STEPS

Change Servers to a Simplex Configuration

When to use

Use this task to change servers in a Disaster Recovery configuration to a simplex configuration.

Related information

See the following topic in this document:

- "Disaster Recovery Concepts" (p. 20-2)

Before you begin

Ensure that the following has occurred before you begin this task:

- The application on both servers is shut down completely.
- All replicated files system are unmounted.

Task

Complete the following steps to change servers in a Disaster Recovery configuration to a simplex configuration.

1 Enter the following command to verify that the application is down on both servers and that all replicated file systems are unmounted:

```
bdf | grep dbdg | wc -l
```

Result: The returned value is 0.

If the returned value is not 0, stop this task and go to "Stop the Platform" (p. 9-7) task.

2 Log in to the active server as `root`.

Use the following command lines to stop replication. Ignore the WARNING but pay attention to any ERROR messages.

```
vradmin -f -g dbdg stoprep dbdg_rvg name_of_server_B
answer y to Continue with stoprep (y/n)? y
vradmin -g dbdg delsec dbdg_rvg name_of_server_B
vradmin -f -g dbdg delpri dbdg_rvg
```

3 On both the active and the standby servers, use the following command to verify if replication is cleared:

```
vradmin printrvg
```

Result: Nothing should be returned on both servers.

4 On the standby (B) server, login as **`root`**.

Enter the following command to update the database and make it active:

```
/opt/lucent/platform/bin/rep_db_reset
```

Press [Enter] to take the default value.

Press [Enter] again.

Result: The following message appears when the database has finished being updated and is made active:

```
rep_db_reset successfully completed.
```

5 On both servers, enter the following command lines to save a copy of the existing sys_config:

```
cd /etc/opt/lucent/platform

cp -p sys_config sys_config.DR
```

6 On both servers, modify the **sys_config** file (**/etc/opt/lucent/platform/sys_config**) to make them both simplex. The contents of the files should be similar to the following:

```
system_install_type=simplex

system_logical_name=<the logical name of the system>

system_role=n/a

remote_system_name=n/a

dynamic_ip=n/a
```

Note: The content **`system_logical_name=<the logical name of the system>`** should not be changed or updated.

Result: Both servers are now independent of each other.

7 Bring the application up on each server or perform an upgrade if needed.

END OF STEPS

21 High Availability

Overview

Purpose

This chapter explains the concepts and provides the tasks that are needed for the High Availability feature.

Contents

High Availability Concepts

High Availability definition

The High Availability feature is a OMS configuration that includes a pair of OMSs (management systems) that communicate with northbound Operations Support Systems (OSSs) to protect against system, site, and communication link failures.

These management systems communicate with two northbound operations support systems (OSSs), which are the following:

- a "Provisioning OSS" (p. 21-2)
- a "Maintenance OSS" (p. 21-2)

High Availability supported platforms

High Availability is supported on the *Server Platforms*. High Availability is not supported on the *PC Platform*.

High Availability licensing

High Availability is an optional licensed feature that is only available to customers who have purchased and installed this feature. The successful operation of the High Availability feature requires the "OMS_HOTDR license" (p. 5-8) . If the High Availability license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

Provisioning OSS

The provisioning OSS communicates with the management system via a TMF814 Northbound interface and it ensures that an active TMF814 Northbound connection exists to both OMSs.

The provisioning OSS determines which management system to send provisioning commands to in order to create network connections; and, by so doing, it defines the management system that receives its commands as the *primary active* and the other as the *secondary active*. In addition, the provisioning OSS defines one management system to be used for NE backups and restores.

The provisioning OSS stores only connection names and it inventories any connections names that lower level systems report that do not exist in the OSS database.

The provisioning OSS is responsible for dropping duplicate notifications.

Note that in general, the High Availability feature only supports the functions that the Northbound TMF814 interface supports.

Maintenance OSS

The maintenance OSS is independently connected to one of the management systems. It is responsible for alarm synchronization after the switchover is made to the other management system.

Management system functioning

In a High Availability configuration, the pair of OMSs (the pair) functions as follows:

- The pair do not have any pre-defined roles and are both active at all times; they are *two fully active, independently-operating management systems*. One management system is referred to the *primary active* and the other is referred to as the *secondary active*. The northbound provisioning OSS determines which management system is the primary active.
- The pair have the *same logical name*.
- The pair do not use any *third party data replication software*.
- The pair operate using the *same time zone*. Their timing source is a single server whose protocol is Network Time Protocol (NTP).

- The pair *discover topological links* between the supported NEs, which are the Metropolis® DMXs.
- A *bi-directional communication path* exists between the primary active and secondary active; however, health monitoring between the two OMSs over this communications link does not occur. (If one management system fails to receive data from the other based on the request connection information request, the management system raises an alarm that is sent to the northbound system.)
- A *user-defined timing offset* exists between the pair in order to run the connection request process. When the connection request process is run, one management system requests the other for all new routes that were provisioned or auto-discovered (CIT created), all connection names that were modified, or all connections that were deleted. The management system that requests this information firsts sort the data into chronological order in the following sequence: disconnected connections, modified connections, and newly added connections. It then updates its database with this information and sends object creation/deletion and attribute value change notifications to the northbound OSS. Note this OMS does not send commands to the network related to these updates in its database.
- If, for any reason, the secondary active fails, and communication between the secondary active and the network are subsequently restored, a *manual database synchronization* of the secondary active and the network must be performed.
- The network reports any *loopbacks* that are created on one of the pair to the other.
- Scheduled backups can cause data inconsistencies; refer to "High Availability configurations and scheduled system backups" (p. 10-4) for details.

High Availability installation parameter

The "History Order Storage Time" (p. 6-55) installation parameter can be changed by a NOC administrator via a menu-driven interface program to ensure correct operation of the High Availability software or to optimize its performance. The recommended setting for a High Availability installation is 24 hours.

This installation parameter can be changed by following the procedures in the "Modify an Installation Parameter" (p. 6-167) task.

High Availability files and directories

The HA tool is typically invoked by a cron job, which called **lt_ha_cron_admin** and is located in the **/opt/lucent/platform/bin** directory.

The HA tool can also be run from the **oms** command line. It is located in **/opt/lucent/oms/bin/dataImporter** directory. The HA tool relies on the properties found in the **dataImporter.properties** file, which is located in the **/opt/lucent/oms/bin** directory.

The following directories contain **.xml** files (one per connection) that are to be imported into the system

- **/var/opt/lucent/importData/new**
- **/var/opt/lucent/importData/deleted**
- **/var/opt/lucent/importData/modified**

The following directories contain log files:

- **/var/opt/lucent/logs/oms/dataImporter.log**
- **/var/opt/lucent/logs/oms/jvm3_ha_info.log**

High Availability related platform alarm

The following hot link provides additional information on a platform alarm that is related to the malfunctioning of a High Availability configuration: "HA_COMMUNICATION-_FAIL" (p. 42-18)

Check the High Availability Installation

When to use

Use this task to check the High Availability installation before you begin any other High Availability-related task.

Related information

See the following topic in this document:

- "High Availability Concepts" (p. 21-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to check the installation prior to beginning any High Availability task.

1 Verify that the CORE and management system installation has been completed by logging in as **`root`** and entering the following command:

```
swlist
```

Result: The system outputs a three column table that indicates the software that is installed. Installed on every system are the following products, whose names appear in the first column of the table: `Base-VXVM`, `BUNDLE11i`, `FEATURE11i`, `...`, `LT_BOOTSTRAP`, `ITorbixASP`, and `Oracle`.

2 Enter the following command to validate that the installation has been successfully completed:

```
tail -4 /var/tmp/auto_installer.log
```

Result: The command outputs the following: `AUTO INSTALL COMPLETED .`

3 Verify that the contents of the **/etc/opt/lucent/platform/sys_config** files on both the server A and server B have the following installation parameters specified:

On server A:

```
system_install_type=ha

system_logical_name=<name chosen during installation>
```

```
system_role=primary

remote_system_name=<server B name>
```

On server B:

```
system_install_type=ha

system_logical_name=<name chosen during installation>

system_role=secondary

remote_system_name=<server A name>
```

4 Verify that the contents of the **/etc/opt/lucent/platform/sys_status** file on both server A and server B have the following status specified:

```
system_status=shutdown
```

5 Verify that the **/etc/hosts** and the **/.rhosts** files contain entries for the server A and server B.

6 Enter the following command lines to validate that the HA adaptor is added:

```
cat /etc/opt/lucent/dsname.cfg
```

Result: The command output should return multiple lines. One of the lines should be the following:

```
HA ds008
```

7 Enter the following command to validate that the remote shell and login are enabled:

```
cat /etc/inetd.conf | grep -e "^shell" -e"^login"
```

Result: The command output should return the following two lines:

```
login    stream tcp nowait ...
shell    stream tcp nowait ...
```

8 Enter the following command to verify that the NTP daemon is running:

```
ps -ef|grep xntp
```

Result: The command output should return a line similar to the following:

```
Root 11936    1    0 Dec 12 ?   0:21 /usr/sbin/xntpd
```

9 Enter the following command to verify that the remote shell is enabled and that the date and time are synchronized:

```
date; remsh hostB date
```

10 Verify that **ssh** works between the primary and secondary servers without a password challenge.

On the primary server, input the following command:

```
ssh <secondary server name>
```

Result: If you logged in to the primary server without a password challenge, go to Step 11.

If a password challenge is displayed, some type of **ssh** setup is required. If local security permits .shosts-based authentication between systems, go to "Configure a Secure Shell (SSH)" (p. 9-27).

If .shosts authentication is not permitted, obtain help from local security administrators to set up certificate-based authentication between the primary and secondary servers.

11 Verify that **ssh** works between the secondary and primary servers without a password challenge.

On the secondary server, input the following command:

```
ssh <primary server name>
```

Result: If you are logged in to the primary server without a password challenge, go to Step 13.

12 Once .shosts-based authentication between systems is established, repeat Step 10 and Step 11, which are the steps for **ssh** verification.

Important! Do not go on to Step 13 until **ssh** works in both directions without password challenges.

13 Use the "View the Parameter Settings of an Installation Parameter" (p. 6-165) task to view the settings of the Connection Variables and Order Handling Variables installation parameters. The "CTP Alarm Monitoring" (p. 6-46) parameter (Connection Variables) must be set to **All**. The "History Order Storage Time" (p. 6-55) parameter (Order Handling Variables) must be set to **24 hours**.

Result: A menu of all tunable parameters is displayed.

If the parameter settings must be changed, use the "Modify an Installation Parameter" (p. 6-167) task.

If the parameter settings do not have to be changed, go to the next step.

END OF STEPS

Initiate High Availability

When to use

Use this task to initiate High Availability.

Related information

See the following topics in this document:

- "High Availability Concepts" (p. 21-1)
- "View the Parameter Settings of an Installation Parameter" (p. 6-165)
- "Modify an Installation Parameter" (p. 6-167)
- "Start the Platform" (p. 9-5)

Before you begin

Verify that the High Availability pair of management systems can communicate, that they were configured at installation time as a High Availability configuration, and that they have the same logical name and time zone.

In addition, make sure the management system is not doing a Database Synchronization operation and that Connection Auto Discovery is not running.

The ha_initialise tool enables you to modify the interval of the cron job in increments of 10, 20, or 30 minutes, with a default interval of 20 minutes. The corresponding new interval and offset interval must be applied manually on the other management system with respect to the management system on which the new values are applied. The offset equals the cron job interval/2.

Example: If the interval of the cron job is set to the default, which is 20 minutes, then the offset between the two servers is 10 minutes. One server is set to 00, 20, and 40; the other server is set to 10, 30, and 50. For further clarification, see the **Results** sections of Step 5 and Step 7 in this task.

Once the tool completes successfully, a message indicates that the HA pair is correctly configured and the cron jobs are started on both machines.

Task

Complete the following steps to initiate High Availability.

1 Use the "Start the Platform" (p. 9-5) to start the application on both server A and server B.

2 Ensure that the servers are synchronized with the network.

3 Log in to server A, which must be the “primary system” to run ha_initialise, as **root**.

4 Enter the following command to start ha_initialise:

```
/opt/lucent/platform/bin/ha_initialise
```

Result: The ha_initialise tool checks several preconditions. If all preconditions are met, you are prompted for values to use for the execution interval that is associated with the cron entries for the **dataImporter** tool. The offsets are automatically calculated using **user selection / 2** and the cron entries on server B are also automatically updated.

5 Enter the following command to verify that the HA cron tool has been created:

```
crontab -l oms|grep Importer
```

Result: Output similar to the following is displayed:

```
00,20,40****/opt/lucent/platform/bin/lt_cron_wrapper -s/opt/lucent/
   oms/bin/dataImporter>/dev/null 2>&1
```

6 Log in to server B as **root**.

7 Enter the following command to verify that the HA cron tool has been created:

```
crontab -l oms|grep Importer
```

Result: Output similar to the following is displayed:

```
10,30,50****/opt/lucent/platform/bin/lt_cron_wrapper -s/opt/lucent/
   oms/bin/dataImporter>/dev/null 2>&1
```

END OF STEPS

Disable the HA cron

When to use

Use this procedure to disable the HA cron job from both server A and server B.

Related information

See the following topic in this document:

- "High Availability Concepts" (p. 21-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to disable the HA cron job.

1 Log in to either server A or server B (but not both servers) as **root**.

2 Enter the following command to invoke the cron job:

```
/opt/lucent/platform/bin/lt_ha_cron_admin
```

3 To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed along with the prompt to `Press [ENTER] to continue`.

4 Press **Enter** to disable the remote system.

5 Enter **q** and press **Enter** to exit the tool.

Result: The HA cron job is disabled on both server A and server B.

END OF STEPS

22 Connection Auto Discovery

Overview

Purpose

This chapter contains conceptual information and the appropriate tasks to support the Connection Auto Discovery command-line tool.

Contents

Connection Auto Discovery Concepts

Connection Auto Discovery definition

The Connection Auto Discovery is a command-line tool that enables users to discover connections that terminate on and pass through NEs that are under the management system control. When Connection Auto Discovery discovers connections that terminate on WAN ports, it creates a Virtual Concatenation Group (VCG). The tool discovers individual connections until it can no longer find link connections or cross connections. It discovers connections based on the database records of existing *uncorrelated* cross connections.

Connection Auto Discovery is designed to find infrastructure connections prior to the discovery of lower rate connections that could be riding on the infrastructure connection. As such, it is possible that the infrastructure orders might not complete before the tool discovers the lower rate connections; thus, the lower rate connections are not discovered. To ensure that all lower rate connections are discovered, we suggest running the tool twice, with a five minute delay between runs.

Connection Auto Discovery supported platforms

Connection Auto Discovery is supported on the *Server Platforms*. Connection Auto Discovery is also supported on the *PC Platform*.

Connection Auto Discovery licensing

The Connection Auto Discovery tool is part of the “OMS_CORE license” (p. 5-5). A separate license is not needed to execute the tool.

Connection Auto Discovery modes of execution

Connection Auto Discovery can be executed through the following modes:

- On-demand via the command line by executing the tool or by executing the tool with its interactive mode; refer to the “On-Demand Execution of Connection Auto Discovery ” (p. 22-9) task for details.
- Scheduled via a cron job; refer to the “Schedule the Connection Auto Discovery Command-Line Tool” (p. 22-13) task for details.

Connection Auto Discovery log files

Each run of Connection Auto Discovery produces a separate set of log files that are located in the following directory:

/var/opt/lucent/logs/oms/tools/auto-discovery

These log files are not accessible from the user interface.

Connection Auto Discovery and the User Activity Log

After it has discovered and validated a new connection, Connection Auto Discovery sends all information relative to the connection to the management system, which performs additional validations and records a success message in the User Activity Log. The User Activity Log indicates the connection name of the discovered connection.

For the installation parameter related to the User Activity Log, see "Enable User Activity Log" (p. 6-13).

For platform alarms related to the User Activity Log, see "UTL_FULL" (p. 42-27) and "UTL_NEARLY_FULL" (p. 42-27).

Connection Auto Discovery and inconsistent connections

The Connection Auto Discovery tool can be enabled when a new connection conflicts with an existing inconsistent connection. Through on or off assignments that are made in the properties file of the tool, users can check for any existing inconsistent connection:

- When the checking is turned on, after finding a new path and before creating a new order, the Connection Auto Discovery verifies if any port involved in the end cross-connections of the newly discovered connection is in the route of an existing inconsistent connection.

  The tool further verifies if the original inconsistent connection has been created via one of the following methods:

  – If the original inconsistent connection has been created via a user and/or a northbound system, the tool does not create an order. It logs an error to indicate that an existing connection shares common ports in the route with the newly discovered connection.

  – If the original inconsistent connection has been system created, the tool performs a database deletion of the original inconsistent connection and it logs an entry to indicate that an inconsistent connection has been deleted. The tool ends.
- When the checking is turned off, the tool continues to create an order for the newly discovered connection.

Connection Auto Discovery and internal VC-4 connections

The Connection Auto Discovery tool can discover internal VC-4 connections even if the parameter setting in the properties file of the tool is set to otherwise; meaning if the `tool.autodiscover.SingleNodeConnectionCreation` parameter in the **autodiscovery.properties** file can be set to no.

Connection Auto Discovery and supported connection rates

The Connection Auto Discovery tool supports the discovery of the following connection rates:

- STS-1/ HO-VC-3
- STS-3c/ VC-4
- STS-12c/ VC-4-4c
- STS-48c/ VC-4-16c
- STS-192c/ VC-4-64c
- VT-1.5/ VC-11 and VT-2/VC-12
- VCG
- LO-VC-3
- OC-48 MS, OC-192 MS, and OC-768 MS
- STM-16 MS, STM-64 MS, and STM-256 MS
- OC-48 RS, OC-192 RS, and OC-768 RS
- STM-16 RS, STM-64 RS, and STM-256 RS
- OCH
- ODU10G
- OMS

Maximize the use of Connection Auto Discovery

To maximize its benefits, Connection Auto Discovery should be run soon after a Network Database Synchronization is completed. See the *OMS Network Element Management Guide* and/or the *OMS Ethernet Management Guide* for more information on Network Database Synchronizations.

In addition, since Connection Auto Discovery examines the live OMS database, if any actions (such as Connection Provisioning) occur on the system while the Connection Auto Discovery is being executed, inaccurate information can be reported; therefore, we recommend that Connection Auto Discovery should be executed when the network is *quiet*.

Edit autodiscovery.properties to Enable the Discovery of Single Node Connections

When to use

Use this task to edit the **autodiscover.properties** file in order to enable the discovery of single node connections.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to edit the **autodiscover.properties** file in order to enable the discovery of single node connections.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /opt/lucent/oms/bin
```

3 Enter the following command to invoke the vi editor and to edit the **autodiscover.properities** file:

```
vi autodiscover.properties
```

4 Change the value of **no** to **yes** in the following line:

```
tool.autodiscover.SingleNodeConnectionCreation= yes
```

5 Enter the following command to save the changes made to the file and to exit the file:

```
<Shift> ZZ
```

Result: The **autodiscover.properities** file has been changed in order to enable the discovery of single node connections.

END OF STEPS

Edit autodiscovery.properties to Limit the Number of Discovered Connections

When to use

Use this task to edit the **autodiscover.properties** file in order to limit the number of connections that can be discovered when running the tool in interactive mode.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to edit the **autodiscover.properties** file in order to limit the number of connections that can be discovered when running the tool in interactive mode.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /opt/lucent/oms/bin
```

3 Enter the following command to invoke the vi editor and to edit the **autodiscover.properities** file:

```
vi autodiscover.properties
```

4 Change the value of **3000** to a lesser number in the following line:

```
tool.autodiscover.ConnNumberLimitInOneRun=3000
```

5 Enter the following command to save the changes made to the file and to exit the file:

```
<Shift> ZZ
```

Result: The **autodiscover.properities** file has been changed in order to to limit the number of connections that can be discovered when running the tool in interactive mode.

END OF STEPS

On-Demand Execution of Connection Auto Discovery

When to use

Use this task to perform an on-demand execution of the Connection Auto Discovery command-line tool.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)
- "Schedule the Connection Auto Discovery Command-Line Tool" (p. 22-13)

Before you begin

The management system database must be synchronized with the network. If needed, perform a database synchronization before you perform this task. See the *OMS Network Element Management Guide* and/or the *OMS Ethernet Management Guide* for database synchronization details. In addition, the OMS database manager must be running.

The Connection Auto Discovery command-line tool can be executed on demand with default options (meaning, without specifying any options) or with an interactive mode option that would enable you to select a particular SONET/SDH rate.

In addition, the Connection Auto Discovery command-line tool can also be scheduled for execution with a cron job; see the "Schedule the Connection Auto Discovery Command-Line Tool" (p. 22-13) task for details.

Task

Complete the following steps to run the Connection Auto Discovery command-line tool.

1 From the machine on which the management system is running, log in as **`oms`**.

2 To execute the tool with its default mode of execution, go to Step 3.

To execute the tool with its interactive mode of execution, go to Step 4.

3 To execute the tool with its default mode of execution, enter the following command from any directory at the prompt:

```
AutoDiscover
```

Result: The Connection Auto Discovery command-line tool is started. When it completes execution, the UNIX® prompt is returned.

4 To execute the tool with its interactive mode of execution, enter the following command from any directory at the prompt:

```
AutoDiscover -i
```

Result: The Connection Auto Discovery command-line tool will prompt you to select a particular SONET/SDH rate. When it completes execution, the UNIX® prompt is returned.

END OF STEPS

View the Results of Connection Auto Discovery

When to use

Use this task to view the results of Connection Auto Discovery.

Related information

See the following topic in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)

Before you begin

The Connection Auto Discovery command-line tool must have been executed.

Task

Complete the following steps to view the results of the Connection Auto Discovery off-line tool:

1 From the machine on which the management system is running, log in as `oms`.

2 Enter the following command to change directories:

```
cd /var/opt/lucent/logs/oms/tools/auto-discovery
```

Result: The directory is changed.

3 Enter the following command to list the log files:

```
ls
```

Result: The log files are listed.

4 Look for the appropriate output file by examining the date and time attached to each filename. The date and time, which represent exactly when the tool was executed, are formatted as a 4-digit year, 2-digit month number, 2-digit date of the month, 2-digit hour (in 24-hour format), 2-digit minutes and 2-digit seconds:

- activityLog.year.month.date.hour.min.sec
- discoveredConnectionLog.year.month.date.hour.min.sec
- discoveredVCGConnectionLog.year.month.date.hour.min.sec
- discrepancyConnectionLog.year.month.date.hour.min.sec
- errorLog.year.month.date.hour.min.sec

Result: The files are displayed.

5 Use any UNIX® tool, such as **vi** or **more**, to view the contents of the particular file.

Result: The logs contain the following information:

- The **Error Log** logs error messages.
- For each discovered connection, the **Discovered Connection Log** gives the Connection Name, Connection Rate, A NE, A port, Z NE, and Z port.
- For each discovered VCG, the **Discovered VCG Log** gives the Connection Name, Connection Rate, A NE, A port, Z NE, and Z port.
- Before discovering Connections, Connection Auto Discovery logs all improper disconnected connections in the **Log of Improper Disconnected Connections**.
- The **Activity Log** gives the starting and finishing time of the procedure and lists the rates of all cross connections assigned to the appropriate connections.

6 View the list of orders (Connection Names) that the management system creates after Connection Auto Discovery is run in the User Activity Log. See the *OMS Network Element Management Guide* for details on how to view the User Activity Log.

END OF STEPS

Schedule the Connection Auto Discovery Command-Line Tool

When to use

Use this task to schedule the automatic execution of the Connection Auto Discovery command-line tool through the use of a cron job.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)
- "Disable the Automatic Execution of the Connection Auto Discovery Command-Line Tool" (p. 22-15)

Before you begin

The management system must be up and running.

Task

Complete the following steps to schedule the automatic execution of the Connection Auto Discovery command-line tool.

1 From the machine on which the management system is running, log in as **root**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **2**, which is Connection Discovery Tool, and press **Enter**.

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To enable the automatic execution of the audit tool, select **Option 1** and press **Enter**.

Result: The default values for the automatic audit tool execution are shown. The default execution time is *10:00* P.M. and the default frequency is *daily*.

5 If the values shown are acceptable, go to Step 10 to save the changes.

To change the execution time, go to Step 6.

To change the frequency of execution, go to Step 8.

6 To change the execution time from the time shown, enter **1** and press **Enter**.

7 Enter the new time in 24-hour format (for example: 09:00 for 9:00 A.M. and 21:30 for 9:30 P.M.) and press **Enter**.

Result: The newly specified time value is displayed.

8 To change the frequency of execution, enter **2** and press **Enter**.

Result: The frequency options are displayed.

9 Select a frequency among the following:

- If you select **Daily**, go to Step 10.
- If you select **Weekly**, select a day of the week and press **Enter**.
- If you select **Monthly**, select a date of the month and press **Enter**.
- If you select **Fixed Date**, enter the month number (1 through 12), a dash (-), a date of the month (1 through 31) and press **Enter**.

10 To save any changes made, enter **s** and press **Enter**.

Result: Changes made to the automatic execution of the tool are saved and the automatic execution of the tool is scheduled.

11 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the Connection Auto Discovery command-line tool is completed.

END OF STEPS

Disable the Automatic Execution of the Connection Auto Discovery Command-Line Tool

When to use

Use this task to disable the automatic execution of the Connection Auto Discovery command-line tool.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)
- "Schedule the Connection Auto Discovery Command-Line Tool" (p. 22-13)

Before you begin

The management system must be up and running.

Task

Complete the following steps to disable the automatic execution of the Connection Auto Discovery command-line tool.

1 From the machine on which the management system is running, log in as `root`.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **2**, which is Connection Discovery Tool, and press **Enter**:

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed.

5 Select the tool to be disabled and press **Enter.**

Result: A confirmation is displayed to verify that you want to disable the execution of this particular tool.

6 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the Connection Auto Discovery command-line tool is completed.

END OF STEPS

DB Delete Connections Tool

When to use

Use this task to automatically delete connections that are marked as an "inconsistent connection". The DelDiscConn can be run on-demand or scheduled via cron.

Note: This tool is typically needed if the SONET/SDH provisioning is being performed by an external system and OMS only inventories the connections as part of discovery. By deleting these connections, the existing cross-connections are freed up to be used in different connections to be discovered by Auto Discovery and if there are no cross-connections left in the connection, it will not be re-discovered by Auto Discovery.

Related information

See the following topics in this document:

- "Connection Auto Discovery Concepts" (p. 22-2)

Before you begin

The management system must be up and running.

Task

Complete the following steps to automatically delete connections that are marked as an "inconsistent connection".

1 From the machine on which the management system is running, log in as **`root`**.

2 *Optional.*Enter the following command to generate a list of discrepant connections:

```
/opt/lucent/platform/bin/DelDiscConn -g
```

Result: The List of discrepant connections are displayed.

3 Enter the following command to delete discrepant connections:

```
/opt/lucent/platform/bin/DelDiscConn
```

Result: The listed discrepant connections are deleted.

END OF STEPS

Schedule the DB Delete Connections Tool

When to use

Use this task to schedule the automatic execution of the DB Delete Connections tool through the use of a cron job.

Related information

See the following topics in this document:

- "DB Delete Connections Tool" (p. 22-17)
- "Disable the Automatic Execution of the DB Delete Connections Tool" (p. 22-20)

Before you begin

The management system must be up and running.

Task

Complete the following steps to schedule the automatic execution of the DB Delete Connections tool.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **4**, which is Discrepancy Connection DB Deletion Tool, and press **Enter**.

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To enable the automatic execution of the audit tool, select **Option 1** and press **Enter**.

Result: The default values for the automatic audit tool execution are shown. The default execution time is *9:30* P.M. and the default frequency is *daily*.

5 If the values shown are acceptable, go to Step 10 to save the changes.

To change the execution time, go to Step 6.

To change the frequency of execution, go to Step 8.

6 To change the execution time from the time shown, enter **1** and press **Enter**.

7 Enter the new time in 24-hour format (for example: 09:00 for 9:00 A.M. and 21:30 for 9:30 P.M.) and press **Enter**.

Result: The newly specified time value is displayed.

8 To change the frequency of execution, enter **2** and press **Enter**.

Result: The frequency options are displayed.

9 Select a frequency among the following:

- If you select **Daily**, go to Step 10.
- If you select **Weekly**, select a day of the week and press **Enter**.
- If you select **Monthly**, select a date of the month and press **Enter**.
- If you select **Fixed Date**, enter the month number (1 through 12), a dash (-), a date of the month (1 through 31) and press **Enter**.

10 To save any changes made, enter **s** and press **Enter**.

Result: Changes made to the automatic execution of the tool are saved and the automatic execution of the tool is scheduled.

11 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the DB Delete Connections tool is completed.

END OF STEPS

Disable the Automatic Execution of the DB Delete Connections Tool

When to use

Use this task to disable the automatic execution of the DB Delete Connections tool.

Related information

See the following topics in this document:

- "DB Delete Connections Tool" (p. 22-17)
- "Schedule the DB Delete Connections Tool" (p. 22-18)

Before you begin

The management system must be up and running.

Task

Complete the following steps to disable the automatic execution of the DB Delete Connections tool.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **4**, which is Discrepancy Connection DB Deletion Tool, and press **Enter**:

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed.

5 Select the tool to be disabled and press **Enter.**

Result: A confirmation is displayed to verify that you want to disable the execution of this particular tool.

6 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the DB Delete Connections tool is completed.

END OF STEPS

23 Network Inventory Extraction

Overview

Purpose

This chapter explains the concepts and provides the tasks that are needed for the execution of the Network Inventory Extraction Tool.

Contents

Network Inventory Extraction Tool Concepts

Network Inventory Extraction tool overview

The Network Inventory Extraction tool maps OMS data elements to VPIsystems™ format and extracts that data from the management system database so it can be used by the VPItransportMaker™ Capacity Planning Tool for ONNS/ASTN, which is the Optical Network Navigator System/Automatic Switch Transport Network.

Note: The VPItransportMaker™ tool is a network planning and optimization tool for SONET/SDH, optical ring, optical mesh, and hybrid networks with ultra long haul (ULH) and Wavelength Routing and Assignment (WRA) capabilities that is offered by VPIsystems™ company. Its graphic editing features help designers to insert nodes, links, and equipment to define the network map and to specify various parameter options. Detailed network design results are calculated including link capacities, equipment lists by node, assigned wavelength slots, the number of WDM systems, and associated optical amplifiers and regenerators. Results are presented as relational flat files, Extensible Markup Language (XML) files, text documents, and tab activated Excel spreadsheets with histograms and pie charts. Interfaces to third party tools, algorithms and OSS are facilitated with XML files, relational flat files, and algorithm APIs.

Network Inventory Extraction tool supported platforms

The Network Inventory Extraction tool is supported on the *Server Platforms*. The Network Inventory Extraction tool is not supported on the *PC Platform*.

Network Inventory Extraction tool licensing

The Network Inventory Extraction tool is an optional licensed feature that is only available to customers who have purchased and installed this feature. See Chapter 5, "Licensing" for details. The successful operation of the Network Inventory Extraction tool requires the "OMS_NETINV license" (p. 5-12), which is typically installed during the initial installation of the management system. If the Network Inventory Extraction tool license was not installed during the initial installation of the management system, see the "Add a License" (p. 5-18) task.

Network Inventory Extraction tool and ONNS considerations

When installing the management system, the value for the "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter should be set to YES so stale Optical Network Navigator System (ONNS) paths are periodically retrieved. If this parameter is set to NO, all stale ONNS paths are retrieved when the Network Inventory Extraction tool is executed, which can take a while to complete.

Network Inventory Extraction tool files generated

The Network Inventory Extraction tool generates a set of VPIsystems™ files in tab separated value (TSV or **.tsv**) format. One file is generated for each data type. The following VPIsystems™ **.tsv** files are stored in **/var/opt/lucent/network_inventory**:

- **Nodes.tsv**
- **LinksLogical.tsv**
- **TrafficMatrices.tsv**
- **TrafficDemands.tsv**
- **DemandParcels.tsv**
- **Path.tsv**
- **PathLinks.tsv**
- **SRLGFaultTable.tsv**
- **SRLGLinkToFaultMap.tsv**

Data types that the management system does not supply are defaulted to the values that are supplied by the VPIsystems™ company.

Network Inventory port number assignment

The service/port number dedicated to execution of the Network Inventory Extraction tool (network_inventory_extraction) is 9215. This port number can be accessed remotely without logging into the management server. Refer to "Table of management system port assignments" (p. 40-1) for the listing of this service/port number.

Execute the Network Inventory Extraction Tool

When to use

Use this procedure to execute the Network Inventory Extraction tool.

Related information

See the following topic in this document:

- "Network Inventory Extraction Tool Concepts" (p. 23-1)

Before you begin

Verify that the "OMS_NETINV license" (p. 5-12) is installed. In addition, update the routes with detailed information for each control plane network connection by displaying its graphical layout on the management system.

Task

Complete the following steps to execute the Network Inventory Extraction tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to execute the Network Inventory Extraction tool:

```
network_inventory_extraction
```

Result: From the **OMS** login, Network Inventory Extraction tool executes and generates the required VPIsystems™ files, which are time stamped and stored in the following directory:

```
/var/opt/lucent/network_inventory
```

3 Browse to the server name to view the VPIsystems™ **.tsv** files:

```
https://<server name>.<domain name>
```

For example: **`https://largo.lucent.com`**

END OF STEPS

24 Insert/Remove Node

Overview

Purpose

This chapter explains the concepts and provides the tasks that are needed to run the Insert/Remove Node command line tool.

Contents

Insert/Remove a Node into a Ring and/or Multiplex Section Connection Concepts

Insert/Remove a Node tool functioning

For SDH physical network connections, the Insert/Remove a Node command line tool can be used to add a node or remove a node from the command line of the HP® server.

The *Insert a Node* version of the tool enables a new node to be brought under management system control for the first time. The node can be inserted into an existing physical network connection (link) in the existing management system network, which includes configurations in which the link is part of a ring topology.

The node to be brought under management system control can be fully operational and can have assigned, pre-existing cross connections that can be part of an existing, end-to-end network connection scheme within the management system. The management system views these cross connections as uncorrelated. The tool ties the existing NE cross connections with the management system end-to-end connections, which is accomplished by provisioning the NE to maintain continuity of all existing network connections.

The *Remove a Node* version of the tool enables a node to be removed/deleted from an existing physical network connection (link) in the existing management system network, which includes configurations in which the link is part of a ring topology.

In either operating mode, the tool inserts or removes a node in an existing physical network connection and appropriately updates all network level information to be consistent with the new configuration. When inserting a node, the tool provisions the NE to maintain continuity of all existing network connections. When deleting a node from a ring/link, the tool updates the management system database accordingly and verifies that only through cross-connections exist between the two links from which the node is being removed, and prohibits the operation unless that constraint is met.

In either operating mode, we highly advise that you perform a database backup before initializing this tool.

Insert/Remove a Node supported platforms

The Insert/Remove Node tool is supported on the *Server Platforms*. The Insert/Remove Node tool is also supported on the *PC Platform*.

Insert/Remove a Node tool licensing

The Insert/Remove a Node tool is part of the “OMS_CORE license” (p. 5-5). A separate license is not needed to execute the tool.

Insert/Remove a Node tool GUI access

If the “Connection Management user task” (p. 7-9) is enabled in a user's user role profile, that user can access the Insert/Remove a Node tool from the management system GUI rather than from the command line of the server.

Digital connections supported

The Insert/Remove Node tool supports digital connections of the following types:

- 1+1 MSP
- UPSR/SNCP
- BLSR/MSSPRING (2F)
- unprotected

The Insert/Remove Node tool does not support the handling of connections created via a *cross-connection based* provisioning approach. For detailed information about cross-connections, refer to the *OMS Connection Management Guide*.

NEs supported

The Insert/Remove Node tool supports the following NEs:

- DDM-2000 OC3 Multiplexer R15.3
- 1675 Lambda Unite MultiService Switch (MSS) R6.1, R7.0, R8.0
- 1643 ADM MultiService Mux (Compact Shelf) R5.0
  1663 Add Drop Multiplexer (ADMu) R5.0, R5.1
- 1643 Access Multiplexer (AM) R6.1, R7.0
  1643 Access Multiplexer Small (AMS) R6.0, R7.0
  1645 Access Multiplexer Compact (AMC) R8.0, R9.0
  1655 Access Multiplexer Universal (AMU) R2.0, R3.0
- 1665 DMX Access Multiplexer R5.1, R5.2, R6.2
  1665 Data Multiplexer Explore (DMXplore) R2.0, R2.1
  1665 DMXtend Access Multiplexer R3.1, R4.0
- WaveStar® ADM 16/1 R6.2, R7.0, R8.0
  WaveStar® TDM10G (STM-64) R4.0, R5.0
  WaveStar® AM 1 R3.2, R4.0, R5.0
- 1671 Service Connect (SC) R4.0, R6.0.1
- Non-managed NEs

In addition, the Insert/Remove Node tool supports the insertion and the removal of indirectly managed NEs, which includes the following:

- The insertion and the removal of an indirectly managed NE into/from a link in between two directly managed NEs
- the insertion and the removal of a directly managed NE into/from a link in between two indirectly managed NEs.

Important! Users can insert and/or remove a repeater through the existing modify DL feature. The management system does not create any connections terminated on a repeater. The Insert/Remove tool denies any request to insert/remove a repeater to a digital link and instructs users to perform this operation from **Modify DL**. If the user inserts a non-repeater node into to a digital link that has repeaters between the links, the tool issues a warning before it starts the insertion. The warning indicates that users must manually re-add the repeaters to the new DLs from **Modify DL** after the tool completes execution.

The Insert/Remove Node tool does not support the insertion and removal of non-managed NEs or unknown NEs.

The Insert/Remove Node tool does not support the insertion and removal of nodes in the ONNS domain.

ODO support

The Insert/Remove Node tool supports the insertion and remove of a node between a managed NE and an Out-of-Domain Object (ODO).

The following configurations are supported:

- The insertion and/or removal of a LO NE between a LO NE and an ODO. When performing an insertion, the VC-4 is in the dropped mode.
- The insertion and/or removal of a HO NE between a HO NE and an ODO. When performing an insertion, the VC-4 is a *pass through*.
- The insertion and/or removal of a LO NE between a HO NE and an ODO. When performing an insertion, the VC-4 is in the dropped mode.
- The insertion and/or removal of a HO NE between a LO NE and an ODO. When performing an insertion, the VC-4 is a *pass through*.
- The insertion and/or removal of an NE into a 1+1 MSP when one end is an ODO. The to-be-inserted node can be either a directly or indirectly managed NE or a BBOX. It can not be a non-managed *edge* NE (ODO).

Multiplex section connection rates supported

The Insert/Remove Node tool supports multiplex section connections for TDM connections for the rates that are shown in the following table.

For the connections with rates that are shown in the following table, when the original connection between two nodes must be split into two connections, default connection names for these two connections are generated. The connection name format currently installed on the management system is used in the generation of the name.

Supported Multiplex Section Connection Rates for TDM Connections	
SDH	**SONET**
N/A	OC-1 (for the DDM-2000 OC3 Multiplexer)
STM-1	OC-3
STM-4	OC-12
STM-16	OC-48
STM-64	OC-192
STM-256 (for the 1675 Lambda Unite MultiService Switch (MSS) only)	OC-768

Client connection types and rates supported

The Insert/Remove Node tool supports the client connection types and rates that are shown in the following table.

If users choose the Pass through option for the insert node operation, the management system maintains the original names of the connections with the rates that are specified in the following table. If the Drop option is chosen, the management system generates default connection names for connections with the rates that are specified in the following table.

Connection Type	SDH Client Connection Rates	SONET Client Connection Rates
Higher Order	VC-256c VC4-64c VC4-16c VC4-4c VC-4	STS-3c STS-12c STS-48c STS-192c STS-1
Lower Order	VC-3 VC-12	VT1.5
Virtual Concatenation Group (VCG)	VC12-xV VC3-xV VC4-xV	STS-1-xv STS-3c-xv VT1.5xv

Validations performed

The insert/remove node tool validates key components. Before running either tool, prepare for the validations performed and note the following:

- The **NE** be inserted/removed must exist in the management system database. In addition, the user entered NE must be an end node for the multiplex section connection for the TDM connections that the user entered.
- The physical **ports** on the inserted NE must exist in the management system database. The two port names specified cannot refer to the same physical port. They must be available to terminate a multiplex section connection for a TDM connection and cannot be used in any connection provisioned. The ports must have the same rate as the multiplex section connection to which the NE is to be inserted. In addition, the protection type of the ports on the original multiplex section connection must be the same as those on the ports of the NE to be inserted.

- The **multiplex section connection for TDM connections** (multiplex section connection) to be inserted/removed must be of a supported rate; it must be in the In Effect state; and all connections riding on the multiplex section connection must be in the In Effect state.
  For remove node, the connection name entered must be a multiplex section connection, the protection types of the source and sync ports of the multiplex section connections must be the same, and more than two nodes must exist in the network.
- For insert node, if the multiplex section connection to be replaced is part of a **BLSR**, the NE model to be inserted must be compatible with the NE models of the BLSR/MSSPRING. The old BLSR/MSSPRING ring name becomes invalid. The system generates a default BLSR/MSSPRING ring name that can be the same as the old ring name. In addition, VC4 paths do not terminate on the NE to be inserted and the NE is inserted using its 2-line interfaces.
  If the node to be removed is part of a closed BLSR/MSSPRING, the BLSR/MSSPRING is converted into an open-ended BLSR/MSSPRING during the removal process. After successful completion, the BLSR/MSSPRING is re-converted into a closed BLSR/MSSPRING. The old BLSR/MSSPRING ring name becomes invalid. The system generates a default BLSR/MSSPRING ring name or reuses the existing ring name.
- Inserting a node into a multiplex section connection that is part of an automatically created **UPSR/SNCP** or a manually created UPSR/SNCP is accommodated. If the multiplex section connection is part of a manually created UPSR/SNCP ring, the NE must be compatible with this manual subnet. The tool automatically recreates the UPSR/SNCP ring after the creation of the multiplex section connections. If the provisioning fails before the recreation of the ring, users must manually create the ring after running the tool in the recovery mode. If the automatic recreation of the ring fails for other reasons, the tool exits and the previous scenario is followed. In both cases, users are notified that the ring recreation failed in the Error Log. (Refer to "Log files generated" (p. 24-7) for the name/format of the Error Log.)
  If the node to be removed is part of a manually created UPSR/SNCP ring, the tool automatically recreates the UPSR/SNCP ring after the multiplex section connections are recreated. If the provisioning fails before the recreation of the ring, users must manually create the ring after running the tool in the recovery mode.
- The Remove Node tool processes only In-Effect Completed **connections** riding on the multiplex section connections. The tool validates all connections; however, connections that are in the Local Design and Implementation states are not processed, but are listed in the Error Logs for manual clean up. The non-In Effect connections are listed in the Error Log for manual clean up before re-starting the tool. Connections in the planned order step are ignored. If the name of a connection that is not In-Effect is entered, processing stops and the connection is logged the Error Log. If the service connection on both digital links is terminated, the connection is processed for further

validations and the connection is recorded in the Error Log without further processing. (Refer to "Log files generated" (p. 24-7) for the name/format of the Error Log.)
The tool handles all types of connections that can be provisioned via the generic provisioning flows except 1x1, 4F-BLSR, and cross-connection based connections.

- When a node is inserted between a managed NE and an ODO, the Insert/Remove Node tool performs validates the NE and the ports on the particular NE.
  When a node is inserted or removed between a managed NE and an ODO, the Insert/Remove Node tool also validates with the digital link (DL). The original digital link (DL) is replaced by two digital links. For a 1+1 MSP, users must manually create a new ODO NE if an ODO NE does not exist, as well as the termination points (TPs) and the PG on the new ODO. The tool validates that the TP names, the PG, and the rate on the ODO match with those on the to-be-inserted node.

Log files generated

Each time the Insert/Remove Node tool is executed, two sets of log files are generated on the HP® server in the **/var/opt/lucent/logs/oms/tools/insertnode** directory.

- An **Error Log** file is generated for NEs, multiplex section connections, or ports that have failed validations and for VC-4s/STS-1s that could not be processed, which are those VC-4s/STS-1s that were not sent to the order handler. The name of the Error Log file is as follows:
  errorLog.year.month.day.hour.min.sec
- A log of all **processed connections** is generated that lists the connection name, order number, order step, and order status along with the date and time in which the tool completed execution. The name of the processed Connections Log is as follows:
  processedConnectionLog.year.month.day.hour.min.sec

Before the Insert/Remove Node tool executes, the tool verifies that enough space exists in the **/var/opt/lucent/logs/oms/tools/insertnode** directory to create the necessary logs. If insufficient space exists in this directory, the tool terminates and outputs this message:

```
Old log files removed due to space issue
```

In addition, the management system GUI provides a hyperlink in the message zone that enables the user to navigate to the Error Log to determine the outcome of the operation.

Messages logged in the User Activity Log

The success and error messages associated with the Insert/Remove Node tool are logged in the User Activity Log, which is accessible from the management system pages.

The User Activity Log displays the following information:

- User Name: <oms>
- Status: <Success, Failure>

- Activity category: Provisioning
- Object type: Connection
- Object name: Connection ID (which is only displayed for successful execution)
- Activity: Add or DB Delete
- User Interface: Command Line
- Date/Time of Log: <yyyy-mm-dd; hh:mm:ss> (or in a date/time format that is dependent upon the user preferences set)
- Details panel: <detailed failure reason>

In addition, the management system GUI provides a hyperlink in the message zone that enables the user to navigate to the processed connection log to determine the outcome of the operation.

PM and related PM installation parameters

After the Insert/Remove Node has completed an insertion of a node, the tool turns on performance monitoring (PM) for the new end points of the digital link, with the default of 24 hour PM data collection.

The related installation parameters and their setting are the following:

- "24 Hour Collect/Monitor (for Network Connections)" (p. 6-62) is set to **collect**.
- "24 Hour Monitor Type (for Network Connections)" (p. 6-61) is set to **none**.
- "24 Hour Interval (for Network Connections)" (p. 6-62) is set to **1**.

Prepare the Installation for Inserting a Node into a Ring and/or Multiplex Section Connection

When to use

Use this procedure to prepare the installation for inserting a node (NE) into a ring and/or multiplex section connection for TDM connections.

Related information

See the following topics in this document:

- "Insert/Remove a Node into a Ring and/or Multiplex Section Connection Concepts" (p. 24-1)
- "Execute a Cold System Backup from the HP® Server" (p. 10-9)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to prepare the installation for inserting a node (NE) into a ring and/or multiplex section connection.

1 Carefully read "Validations performed" (p. 24-5) and make any appropriate adjustments.

2 For the NE to be inserted, verify the following:

- Verify that the NE to be inserted is installed and the physical fibers are connected.
- Verify that the physical ports are provisioned.
- Verify that protection groups have been provisioned on the ports.
- Verify that any involved NE ports are dormant in order to prevent data discrepancies.
- Verify that the NE is pre-configured to allow the management DCN to reach the node and that DCN connectivity has been established between the management system and the NE.
- For Alcatel-Lucent NEs under management system control, verify that the NE is added to the management system using the Add NE-OS Connections page and that all necessary cross-connections are established.

  Important! Preprovisioning of the cross-connects on the node to be inserted is recommended, but not absolutely needed. If the tool does not find the cross-connects, it sends provisioning commands to the NE. If the provisioning commands fail, recovery data files are created and you can continue processing after the errors are manually resolved.

3 Use the NE CIT to disable the Trail Trace identifiers for Ethernet-over-SDH service that is used by the management DCN.

4 Divert traffic from the multiplex section connection where the NE is to be inserted.

5 If configured, reconfigure TIM at the NE being inserted and at the neighboring NEs. (Note: inserting an NE inhibits alarms and traffic from being sent across the link.)

6 Perform a full database synchronization on the NE to be inserted into the ring.

7 Complete all steps in the "Execute a Cold System Backup from the HP® Server" (p. 10-9) task.

Note: Before you run the tool, the tool warns you to perform a database backup prior to execution and to make sure that the relevant DL does not have any link connections in the **reserved for reinstate** state.

END OF STEPS

Insert a Node into a Ring and/or Multiplex Section Connection

When to use

Use this procedure to insert a node (NE) into a ring and/or multiplex section connection.

Related information

See the following topic in this document:

- "Insert/Remove a Node into a Ring and/or Multiplex Section Connection Concepts" (p. 24-1)
- "Prepare the Installation for Inserting a Node into a Ring and/or Multiplex Section Connection" (p. 24-9)
- "View the Error Log and Connection Log Files" (p. 24-14)
- "Prepare the Installation for Inserting a Node into a Ring and/or Multiplex Section Connection" (p. 24-9)

Before you begin

Step 1 of this task requires you to complete the "Prepare the Installation for Inserting a Node into a Ring and/or Multiplex Section Connection" (p. 24-9) task.

The tool should be run during a quiet time in order to avoid disrupting the flow of existing traffic. Also, to avoid scheduling operations simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

Task

Complete the following steps to insert a node (NE) into a ring and/or multiplex section connection.

1 Complete all steps in "Prepare the Installation for Inserting a Node into a Ring and/or Multiplex Section Connection" (p. 24-9) task.

2 From the machine on which the management system is running, log in as `oms`.

Result: The tool warns you to perform a database backup prior to execution and to make sure that the relevant DL does not have any link connections in the **reserved for reinstate** state.

3 Enter the following command to invoke the tool:

```
OmsInsertNode
```

4 At the prompt, specify if the running of **OmsInsertNode** is a new run or a recovery from a previous file run.

For a new run, go to step Step 5.

For a recovery, go to step Step 7.

5 For a new run, specify the following:

- The NE name of the node being inserted.
- The connection name of the multiplex section connection in which the node will be inserted.
- The Port A and Port Z IDs of the node to be inserted.
- The in-effect VC-4/STS1 connections (generated by the system) that should be passed-through or dropped. For dropped connections, enter the end port information. (Note: Unprotected structured VC-4/STS-1 connections can be passed through or dropped. Protected structured VC-4/STS-1 connections are automatically passed-through.)
- For certain NEs, the cross-connection port information to create internal VC-4/STS-1 cross-connects.

Result: The tool validates the existence of an insert node recovery data file. If a recovery data file does not exist, the tool continues execution. If a recovery data file exists, the tool exits with the following output: `Recovery data file exists - please re-run the tool in the Recovery mode`. Go to step Step 7.

If the tool executes and all validations are successful, the tool drops the VC-4/STS-1 connections that need to be dropped and provisions through connections for use in VC-12s or VC-3s/Vt1.5s as determined from the management system database. It updates the database to reflect the new configuration. The connections are passed to the order handler where In Effect orders are created. A message is subsequently stored in the User Activity Log. In addition, the tool turns on performance monitoring (PM) for the new end points of the digital link, with the default of 24 hour PM data collection.

If the tool executes and the provisioning of connections fail, an order is not created for the connection. The tool logs the connection in the Error Log, saves the processed connections data and status in a recovery data file, and exits. Go to Step 6.

6 If provisioning the connections has failed during a new run of **OmsInsertNode**, log in to the management system and rectify any problems. Access the connections list, and based on the Error Log information, resolve any discrepancies and move the connection to In Effect. Go to Step 3 to restart the process.

7 For a recovery run, input is not required because the **OmsInsertNode** tool starts processing from the previously failed connection.

> **Result:** If the provisioning fails again during this recovery run, the new recovery data is saved into a recovery data file that overwrites the previous recovery data file.

8 Once the tool has successfully completed, use the CIT to enable trail trace identifiers for Ethernet-over-SDH service if they are used.

END OF STEPS

View the Error Log and Connection Log Files

When to use

Use this procedure to view the Error Log (**errorLog**) and the Connection Log (**ConnectionLog**) files that are created during an iteration of the Insert/Remove Node tool.

Related information

See the following topic in this document:

- "Insert/Remove a Node into a Ring and/or Multiplex Section Connection Concepts" (p. 24-1)

Before you begin

Executing the **OmsInsertNode** tool generates the Error Log and the Connection Log; therefore, the "Insert a Node into a Ring and/or Multiplex Section Connection" (p. 24-11) task must be run first.

Task

Complete the following steps to view the Error Log and Connection Log files that are created during an iteration of the Insert/Remove Node tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /var/opt/lucent/logs/oms/tools/insertnode
```

3 Enter following command to access the Connection Log with the **vi** editor:

```
vi ProcessedConnectionLog.<year.month.day.hour.min.sec>
```

Result: The editor enables you to view the file.

4 Enter the following command to exit the file:

```
Shift <ZZ>
```

Result: The system puts you back at the command line.

5 Enter following command to access the Error Log with the **vi** editor:

```
vi errorLog.<year.month.day.hour.min.sec>
```

Result: The editor enables you to view the file.

6 Enter the following command to exit the file:

```
Shift <ZZ>
```

Result: The system puts you back at the command line.

END OF STEPS

Remove a Node from a Ring and/or Multiplex Section Connection

When to use

Use this procedure to remove a node (NE) from a ring and/or multiplex section connection.

Related information

See the following topics in this document:

- "Insert/Remove a Node into a Ring and/or Multiplex Section Connection Concepts" (p. 24-1)
- "Execute a Cold System Backup from the HP® Server" (p. 10-9)
- "Table of scheduled activities" (p. 41-4)

Before you begin

We highly advise that you perform a database backup before initializing this tool with the "Execute a Cold System Backup from the HP® Server" (p. 10-9) task.

The tool should be run during a quiet time in order to avoid disrupting the flow of existing traffic. Also, to avoid scheduling operations simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

The tool performs updates in the following order: multiplex section connections for TDM connections, VC4-4c, VC4-16c, VC4-64c, VC-4 paths, and lower order paths.

Task

Complete the following steps to remove a node (NE) from a ring and/or multiplex section connection.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command to invoke the tool:

```
OmsRemoveNode
```

3 At the prompt, specify if the running of **OmsRemoveNode** is a new run or a recovery from a previous file run.

For a new run, go to Step 4.

For a recovery, go to Step 6.

4 For a new run, specify the following:

- The NE name of the node being removed.
- The connection name of the two multiplex section connections from where the node is to be removed.

Result: The tool validates the existence of a remove node recovery data file. If a recovery data file does not exist, the tool continues execution. If a recovery data file exists, the tool exits with the following output:

`Recovery data file exists - please re-run the tool in the Recovery mode`. Go to step Step 6.

If the tool executes and all validations are successful, the connection is passed to the order handler where an In Effect order is created for the connection. A message is subsequently stored in the User Activity Log.

If the tool executes and the removal of connections fail, an order is not created for the connection. The tool logs the connection in the Error Log, saves the processed connections data and status in a recovery data file, and exits. Go to Step 5.

5 If removing the connections has failed during a new run of **OmsRemoveNode**, log in to the management system and rectify any problems. Access the connections list, and based on the Error Log information, resolve any discrepancies and move the connection to In Effect. Go to Step 2 to restart the process.

6 For a recovery run, input is not required because the **OmsInsertNode** tool starts processing from the previously failed connection.

Result: If the provisioning fails again during this recovery run, the new recovery data is saved into a recovery data file that overwrites the previous recovery data file.

END OF STEPS

25 NE In-Service Upgrade

Overview

Purpose

This chapter explains the concepts and provides the tasks that are needed for the execution of the NE In-Service Upgrade command-line tool. This tool is currently only available for the 1675 Lambda Unite MultiService Switch (MSS).

Contents

NE In-Service Upgrade Concepts

NE In-Service Upgrade tool functional description

For the 1675 Lambda Unite MultiService Switch (MSS), low order switching is provided through an optional circuit pack, which users can add at any time to an in-service NE. To accommodate the generation of low order link connections (LCs) and contained termination points (CTPs) based on the interface standard of this particular circuit pack, the management system provides users with the NE In-Service Upgrade tool.

The NE In-Service Upgrade tool enables the generation of the required VT1.5 link connections for SONET and the low order VC-3 and VC-12 link connections for SDH.

Note: Check the "Summary of supported NEs" (p. 1-5) to determine if this particular NE is supported in this release of the management system.

NE In-Service Upgrade tool supported platforms

The NE In-Service Upgrade tool is supported on the *Server Platforms*. The NE In-Service Upgrade tool is not supported on the *PC Platform*. The PC Platform does not support TL1 NEs.

NE In-Service Upgrade tool licensing

The NE In-Service Upgrade tool is part of the "OMS_CORE license" (p. 5-5) . A separate license is not needed to execute the tool.

NE In-Service Upgrade tool operational scenario

The following operational scenario occurs prior to the execution and during the execution of the NE In-Service Upgrade tool:

- The NE is added to the system, is synchronized, and some high order service connections can be provisioned.
- The optional, low order switching circuit pack is installed into an in-service NE, which currently is the 1675 Lambda Unite MultiService Switch (MSS).
- The tool creates a set of log files and performs its necessary equipment and link verifications. It recognizes the circuit pack, adds its particulars to the equipment list, and issues the "LO_UPGRADE_REQUIRED" (p. 42-19) persistent alarm, which in effect, instructs the user to run the NE In-Service Upgrade tool manually to generate low order link connections (LCs) and contained termination points (CTPs.) Any errors are written to the log files.
- The user acknowledges the "LO_UPGRADE_REQUIRED" (p. 42-19) alarm and runs the NE In-Service Upgrade tool from the command line.
- The tool prepares a list of NEs to be processed along with a list of connections on the NE. It verifies that the NE at the far end is equipped with a compatible low order switching circuit pack. If the far NE is so equipped, it generates the appropriate low order link connections (LCs) and creates the CTPs. Once all low order LCs and CTPs are generated, the tool clears the persistent alarm. The tool repeats this step for the next NE. Any errors are written to the log files.

NE In-Service Upgrade tool considerations

The following considerations should be taken into account when executing the NE In-Service Upgrade tool:

- Once the low order switch fabric is established as the SONET or SDH interface standard, it cannot be changed.
- The low order switch fabric can only be added to the NE; it cannot be removed or deleted.
- CTPs are generated only when link connections are generated.

- All NEs that are marked with discrepancy errors—meaning, the low order cross-connection capability exists, but the low order link connections and CTPs have not been generated—are processed under one execution request.
- The tool does not accommodate the Insert/Remove Node command-line tool.

NE In-Service Upgrade tool log files

The NE In-Service Upgrade tool creates an error log file and an activity log file in the following directory:

/var/opt/lucent/logs/oms/tools/ne-inservice-upgrade

The names of the log files includes the date and time of the creation.

Examples:

/var/opt/lucent/logs/oms/tools/errorLog.year.month.day.hour.min.sec

/var/opt/lucent/logs/oms/tools//activityLog.year.month.day.hour.min.sec

NE In-Service Upgrade tool execution

The NE In-Service Upgrade tool should be executed when the management system is lightly loaded because is can cause a large amount of processing and numerous database updates if a quantify of NEs are to be processed.

The tool can be manually executed on demand from the command-line or it can be scheduled to run as a cron job. To execute the tool on demand from the command line, see the "Run the NE In-Service Upgrade Tool from the Command Line" (p. 25-4) task.

NE In-Service Upgrade related platform alarm

The following hot link provides additional information on a platform alarm that is related to the NE In-Service Upgrade: "LO_UPGRADE_REQUIRED" (p. 42-19).

Run the NE In-Service Upgrade Tool from the Command Line

When to use

Use this task to run the NE In-Service Upgrade Tool from the command line.

Related information

See the following topic in this document:

- "NE In-Service Upgrade Concepts" (p. 25-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to run the NE In-Service Upgrade tool from the command line.

1 From the machine on which the management system is running, log in as **`oms`**.

Result: You are now logged in as **`oms`**.

2 Enter the following command to execute the NE In-Service Upgrade tool:

```
NEInServiceUpgrade
```

Result: The tool performs the upgrade and generates the required VT1.5 link connections (LCs) for SONET.

END OF STEPS

Schedule the NE In Service Upgrade Tool

When to use

Use this task to schedule the automatic execution of the NE In Service Upgrade tool through the use of a cron job.

Related information

See the following topic in this document:

- "NE In-Service Upgrade Concepts" (p. 25-1)

Before you begin

The management system must be up and running.

Task

Complete the following steps to schedule the automatic execution of the NE In Service Upgrade tool.

1 From the machine on which the management system is running, log in as `root`.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **3**, which is NE In Service Upgrade Tool, and press **Enter**.

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To enable the automatic execution of the tool, select **Option 1** and press **Enter**.

Result: The default values for the automatic tool execution are shown. The default execution time is *00:00* A.M. and the default frequency is *weekly on Monday*. The recommended execution time is between 00:00 A.M. and 02:00 A.M.

5 If the values shown are acceptable, go to Step 10 to save the changes.

To change the execution time, go to Step 6.

To change the frequency of execution, go to Step 8.

6 To change the execution time from the time shown, enter **1** and press **Enter**.

7 Enter the new time in 24-hour format (for example: 09:00 for 9:00 A.M. and 21:30 for 9:30 P.M.) and press **Enter**.

Result: The newly specified time value is displayed.

8 To change the frequency of execution, enter **2** and press **Enter**.

Result: The frequency options are displayed.

9 Select a frequency among the following:

- If you select **Daily**, go to Step 10.
- If you select **Weekly**, select a day of the week and press **Enter**.
- If you select **Monthly**, select a date of the month and press **Enter**.
- If you select **Fixed Date**, enter the month number (1 through 12), a dash (-), a date of the month (1 through 31) and press **Enter**.

10 To save any changes made, enter **s** and press **Enter**.

Result: Changes made to the automatic execution of the tool are saved and the automatic execution of the tool is scheduled.

11 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the NE In-Service Upgrade tool is completed.

END OF STEPS

Disable the Automatic Execution of the NE In-Service Upgrade Tool

When to use

Use this task to disable the automatic execution of the NE In-Service Upgrade tool.

Related information

See the following topic in this document:

- "NE In-Service Upgrade Concepts" (p. 25-1)

Before you begin

The management system must be up and running.

Task

Complete the following steps to disable the automatic execution of the NE In Service Upgrade tool.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to execute the scheduling tool:

```
/opt/lucent/platform/bin/lt_cronadmin
```

Result: The scheduling tool is started.

3 Select Option **3**, which is NE In Service Upgrade Tool, and press **Enter**:

Result: The current setting of the automatic execution is displayed as an entry in the UNIX® crontab format.

4 To disable the automatic execution of the tool, select **Option 2** and press **Enter**.

Result: The current schedule of the automatic executions are displayed.

5 Select the tool to be disabled and press **Enter.**

Result: A confirmation is displayed to verify that you want to disable the execution of this particular tool.

6 Enter **q** and press **Enter** to return to the main screen, and then **q** and press **Enter** to exit the scheduling tool.

Result: The automatic execution of the NE In-Service Upgrade tool is completed.

END OF STEPS

26 1625 LambdaXtreme® Transport DWDM Upgrade and Merge

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the DWDM Upgrade and Merge command-line tools for 1625 LambdaXtreme® Transport NEs.

Contents

DWDM Uprade and Merge Concepts

DWDM Upgrade and Merge definition

Dense Wavelength Division Multiplexing (DWDM) Merge is a set of two in-service command-line tools that enables customers who have 1625 LambdaXtreme® Transport to upgrade existing One Degree and Two Degree Reconfigurable Optical Add/Drop Multiplexers (1D_ROADM and 2D_ROADM DWDM NEs) to 3D_WXC NEs and to merge them into one Wavelength Cross-Connect (WXC) system NE without traffic disruption.

Note: Check the "Summary of supported NEs" (p. 1-5) to determine if this particular NE is supported in this release of the management system.

DWDM Upgrade and Merge tool supported platforms

The DWDM Upgrade and Merge tool is supported on the *Server Platforms*. The DWDM Upgrade and Merge tool is not supported on the *PC Platform*. The PC Platform does not support TL1 NEs.

DWDM Upgrade and Merge tool licensing

The DWDM Upgrade and Merge tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

DWDM Upgrade and Merge tool scenarios and functionality

The DWDM Upgrade and Merge command-line tool can upgrade and merge a 1D_ROADM and a 2D_ROADM to a 3D_WXC.

The upgrade and merge into a single NE, with a single target identifier (TID), results in the following:

- One of the two NEs involved in the upgrade/merge loses its identity, which results in the deletion of the TID. This NE is referred to as the *subordinate node*.
  The other NE, which the subordinate node is merged to, is equipped with the required mesh packs. This NE is referred to as the *master node*.
  Important! The TID of the master node and the port AIDs of the master node cannot be changed in the merge operation.
- The line port(s) (1E for the 1D_ROADM and 1E and 1W for the 2D_ROADM) of the subordinate node are redesignated with 2E (or 2W) if the subordinate node is a 1D_ROADM; or 2E and 2W if the subordinate node is a 2D_ROADM.
- All OT ports associated with the subordinate node are redesignated with their association to the new line ports and with changes to the port addresses because of the re-allocation of shelf names.

Refer to the "Run the DWDM Upgrade Command-Line Tool" (p. 26-4) and "Run the DWDM Merge Command-Line Tool" (p. 26-6) tasks for details.

DWDM Upgrade and Merge requirements

The following requirements pertain to the upgrade/merge of 1625 LambdaXtreme® Transport ROADMs to WXC NEs:

- The tool supports the upgrade of one and the merge of two 1625 LambdaXtreme® Transport NEs at one time, during one iteration of the command-line tool.
- Both the master node and the subordinate node must be from the same type (both of them must be 1625 LambdaXtreme® Transport) and both are of the same product release.
- Both the DWDM NEs and their equipment must be inventoried in management system before the execution of the tool.

- The OS links between two optical transponders (OTs) of the two NEs to be merged must be inventoried as an internal OS link after the upgrade/merge operation, which allows an OS between two OTs.
- The subordinate node that is targeted for deletion cannot be the gateway node for communication with the management system.
- Only OS links interconnect the two 1625 LambdaXtreme® Transport NEs that are being merged, which means that the two nodes are not connected on the high speed side.
- Autonomous notifications are not required for northbound systems from OMS. Any discrepancies in the northbound system(s) after the tool is successfully run have to be reconciled by those system users.
- The optical layer connections from the two 1625 LambdaXtreme® Transport nodes do not have any interconnection to the TDM NEs.
- The optical layer connections and links are updated whether they were provisioned in cross-connect mode or manual mode.

DWDM Upgrade and Merge log files

The DWDM Upgrade tool creates an error log file and an activity file in the following directory:

/var/opt/lucent/logs/oms/tools/LX-node-upgrade

The names of the log files include the date and the time of their creation. For example:

errorLog.yyyy.mm.dd.hh.mm.ss

activityLog.yyyy.mm.dd.hh.mm.ss

The DWDM Merge tool creates an error log file and an activity file in the following directory:

/var/opt/lucent/logs/oms/tools/merge_node

The names of the log files include the date and the time of their creation. For example:

merge_node_activityLog.yyyy.mm.dd.hh.mm.ss

merge_node_errorLog.yyyy.mm.dd.hh.mm.ss

merge_node_processedConnLog.yyyy.mm.dd.hh.mm.ss

Run the DWDM Upgrade Command-Line Tool

When to use

Use this task to run the DWDM Upgrade command-line tool for 1625 LambdaXtreme® Transport NEs.

Related information

See the following topic in this document:

- "DWDM Uprade and Merge Concepts" (p. 26-1)

Before you begin

The master NE itself must be upgraded to the 3D_WXC.

You do not have to bring down the management system in order to run the DWDM Upgrade command-line tool.

The NE to be upgraded must exist in the management system database, but it must deactivated.

Sufficient space must exist to create the necessary log files. The log files require 30Mb.

Task

Complete the following steps to run the DWDM Upgrade command-line tool.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command line to invoke the DWDM Upgrade command line tool:

```
LXNodeUpgrade
```

Result: The tool verifies that enough space exists (30Mb) to create the necessary log files. If enough space exists, the tool begins to execute and prompts you for specific information about the particular NE.

3 When prompted, enter the name of the NE to be upgraded.

4 When prompted, specify the following NE model to which the NE is to be upgraded:

3D_WXC

Result: The DWDM Upgrade tool upgrades the internal NE model from a 1D_ROADM or a 2D_ROADM to a 3D_WXC.

In addition the tool creates a log file. Refer to "DWDM Upgrade and Merge log files" (p. 26-3) for details regarding tool output.

5 Use the following command lines to check the log files to verify the execution of the tool.

```
cat activityLog.yyyy.mm.dd.hh.mm.ss
```

```
cat errorLog.yyyy.mm.dd.hh.mm.ss
```

Results: Correct any errors that are documented in the log files. If you have any difficulties, contact Alcatel-Lucent Customer Support Services. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

END OF STEPS

Run the DWDM Merge Command-Line Tool

When to use

Use this task to run the DWDM Merge command-line tool for 1625 LambdaXtreme® Transport NEs.

Related information

See the following topic in this document:

- "DWDM Uprade and Merge Concepts" (p. 26-1)
- "Run the DWDM Upgrade Command-Line Tool" (p. 26-4)

Before you begin

Read "DWDM Upgrade and Merge requirements" (p. 26-2) carefully before beginning this task.

You do not have to bring down the management system in order to run the DWDM Merge command-line tool.

The **`LXNodeUpgrade`** must have been run on the master node. See "Run the DWDM Upgrade Command-Line Tool" (p. 26-4) for details.

A database synchronization must have been run on the master node.

The two nodes to be merged cannot be connected on the high-speed side.

Verify that the subordinate node is not a Gateway NE (GNE) or an FTAM gateway node. If the subordinate node is a GNE or an FTAM gateway, make sure it is reassigned to some other node and update the appropriate RNEs before running the DWDM Merge tool.

You cannot terminate the execution of the tool during any point while it is running.

Task

Complete the following steps to run the DWDM Merge command-line tool.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command line to invoke the DWDM Merge command line tool:

```
merge_node
```

3 When prompted, enter the TID (target identifier) of the master NE into which you are merging.

Note: the TID must exactly match how it was entered in the management system database.

4 When prompted, enter the TID (target identifier) of the subordinate NE that you want to be deleted after the merge.

Note: the TID must exactly match how it was entered in the management system database.

Result: The TIDs, NE releases, and NE models are verified.

If the TIDs match, the tool updates the records of the subordinate node to that of the master node in the management system database and it deletes all internal OS links in the subordinate node. If the database deletion of the connections and the links fails, you must use manual methods to delete the remaining OS links and the subordinate node.

If the TIDs do not match, the following messages are output:

```
TID <xxx> does not exist in OMS as entered. Please enter
again.
```

```
Both the TIDs do not exist in OMS as entered. Please enter
again.
```

Refer to "DWDM Upgrade and Merge log files" (p. 26-3) for details regarding tool output.

5 Use the following command lines to check the log files to verify the execution of the tool.

```
cat merge_node_activityLog.yyyy.mm.dd.hh.mm.ss
```

```
cat merge_node_processedConnLog.yyyy.mm.dd.hh.mm.ss
```

```
cat merge_node_errorLog.yyyy.mm.dd.hh.mm.ss
```

Results: Correct any errors that are documented in the log files. If you any have difficulties, contact Alcatel-Lucent Customer Support Services. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

End of steps

27 LambdaXtreme® Channel Upgrade

Overview

Purpose

This chapter contains the conceptual information and the related task that are needed to upgrade a number of channels when a 1625 LambdaXtreme® Transport NE is upgraded from R6.0 to R7.0 within the managed domain.

Contents

1625 LambdaXtreme® Transport Channel Upgrade Tool Concepts

1625 LambdaXtreme® Transport Channel Upgrade tool overview

The 1625 LambdaXtreme® Transport Channel Upgrade tool is a command-line tool (tool) that is used to upgrade the number of channels from 64 to 128 when the 1625 LambdaXtreme® Transport version is upgraded from R6.0 to R7.0 within the managed domain. The user must identify the A and/or Z NEs, and the system appropriately updates all link connections.

Note: Check the "Summary of supported NEs" (p. 1-5) to determine if this particular NE is supported in this release of the management system.

1625 LambdaXtreme® Transport Channel Upgrade tool supported platforms

The 1625 LambdaXtreme® Transport Channel Upgrade tool is supported on the *Server Platforms*. The 1625 LambdaXtreme® Transport Channel Upgrade tool is not supported on the *PC Platform*. The PC Platform does not support TL1 NEs.

1625 LambdaXtreme® Transport Channel Upgrade tool licensing

The 1625 LambdaXtreme® Transport Channel Upgrade tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

1625 LambdaXtreme® Transport Channel Upgrade tool functional requirements

The 1625 LambdaXtreme® Transport Channel Upgrade tool adheres to the following functional requirements:

- The user must complete an OMS database before executing this tool. In addition, the user should complete any NE database backups before executing this tool.
- The user does not have to stop the application to run the tool. The tool is run via a command line on the UNIX window of host.
- The user must complete all the necessary re-routing prior to the Channel Upgrade to ensure an in-service upgrade.
- The OMS NE-OS connections to all affected NEs are disabled prior to the upgrading. These connections remain disabled until all upgrades are completed and the Channel Upgrade tool is executed on OMS.
- Upon completing the upgrade on the network and using the Channel Upgrade tool, the connections to the affected NEs are re-enabled, and database resynchronizations are performed to resynchronize the OMS NE configuration data with the NE changes (such as to update CP and port data).
- The Channel Upgrade tool only updates the channel number. Other port parameters are updated automatically via the database synchronization that must occur after the upgrade.
- During the Channel Upgrade process, no other network topology changes; for example, nodes cannot be added to the topological link during the upgrade process.
- The PM parameters and the history alarms on the port remain the same before and after the Channel Upgrade.
- The protection group name will be kept the same by the user.

1625 LambdaXtreme® Transport Channel Upgrade tool log files

The 1625 LambdaXtreme® Transport Channel Upgrade tool creates an error log file and an activity file in the following directory:

```
/var/opt/lucent/logs/oms/tools/channel-upgrade
```

The names of the log files include the date and the time of their creation. For example:

errorLog.yyyy.mm.dd.hh.mm.ss

activityLog.yyyy.mm.dd.hh.mm.ss

The names of the log files include the date and the time of their creation. For example:

lx-channel-upgrade_activityLog.yyyy.mm.dd.hh.mm.ss

lx-channel-upgrade_errorLog.yyyy.mm.dd.hh.mm.ss

Run the 1625 LambdaXtreme® Transport Channel Upgrade tool Command-Line Tool

When to use

Use this task to run the Channel Upgrade command-line tool for 1625 LambdaXtreme® Transport NEs.

Related information

See the following topic in this document:

- "1625 LambdaXtreme® Transport Channel Upgrade Tool Concepts" (p. 27-1)

Before you begin

You do not have to bring down the management system in order to run the Channel Upgrade command-line tool.

Step 1 of this task requires you to back up the management system and the NE databases.

Step 2 of this task optionally instructs you to back up the any the NE databases.

Sufficient space must exist to create the necessary log files. The log files require 30Mb.

Task

Complete the following steps to run the Channel Upgrade command-line tool.

1 Complete the steps in the "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) task to back up the management system.

2 Optionally, backup any applicable NE databases.

3 From the machine on which the management system is running, log in as **oms**.

4 Enter the following command line to invoke the Channel Upgrade command line tool:

```
LXChannelUpgrade
```

Result: The tool verifies that enough space exists (30Mb) to create the necessary log files. If enough space exists, the tool begins to execution. If not enough space exists, the tool attempts to clean up the directory and begin execution.

5 When prompted, enter the A and Z NE names.

Result: The tool verifies the parameters supplied, that the NEs to be upgraded are of the correct type, are deactivated, and are version R7.0. Based on your input parameters, the tool generates new link connections and corresponding CTPs. In addition, it updates the timeslots of the existing link connections and corresponding CTPs between the A and Z NEs.

END OF STEPS

28 TDM NE Optical Lines Upgrade

Overview

Purpose

This chapter explains the concepts and provides the tasks that are needed for the execution of the TDM NE Optical Lines Upgrade command-line tool.

Contents

TDM NE Optical Lines Upgrade Concepts

TDM NE Optical Lines Upgrade tool functional description

The Time Division Multiplexing Network Element (TDM NE) Optical Lines Upgrade command-line tool is used to support an upgrade of optical lines within the managed domain for TDM NEs. These TDM NEs include directly managed NEs and NEs that are managed through a legacy element management system, such as Navis® EMS. Black boxes are also included.

Note: Check the "Summary of supported NEs" (p. 1-5) to determine which TDM NEs are supported in this release of the management system.

The tool supports all SONET and SDH physical network connection rates (that is, all OC-n and STM-n rate physical network connections). Users must identify the A/Z NEs, the A/Z pack names, the A/Z port IDs, and the new rate via the tool, and the management system appropriately updates all connection related configuration information based on the new/higher optical line rate, which includes the appropriate renaming of physical network connections and the updating of ring information.

TDM NE Optical Lines Upgrade tool supported platforms

The TDM NE Optical Lines Upgrade tool is supported on the *Server Platforms*. The TDM NE Optical Lines Upgrade tool is also supported on the *PC Platform*.

TDM NE Optical Lines Upgrade tool licensing

The TDM NE Optical Lines Upgrade tool is part of the "OMS_CORE license" (p. 5-5) . A separate license is not needed to execute the tool.

TDM NE Optical Lines Upgrade tool GUI access

If the "Connection Management user task" (p. 7-9) is enabled in a user's user role profile, that user can access the TDM NE Optical Lines Upgrade tool from the management system GUI rather than from the command line of the server.

TDM NE Optical Lines Upgrade tool operational scenario

The following operational scenario occurs prior to the execution and during the execution of the TDM NE Optical Lines Upgrade tool:

- Prior to running the tool, the user must perform a set of tasks which include a management system database backup and an NE database backup, the disabling of the OMS-to-NE connection on the NE to be upgraded, and the upgrade of the NE according to the NE upgrade manual, which must include all the necessary rerouting to ensure an in-service upgrade.
- User executes the tool and provides the NE name, circuit pack name, and circuit pack slot ID.
- The tool gets the list of connections (digital links) based on the updated physical termination points (PTPs); generates new link connections and the corresponding new contained termination points (CTPs); updates the timeslots of the existing link connections and CTPs; updates the Connection Name, but keeps the same SDH or SONET terminology; and updates the ring rate, ring name, and existing ring parameters.

TDM NE Optical Lines Upgrade tool considerations

The following considerations should be taken into account when executing the TDM NE Optical Lines Upgrade tool:

- The tool supports upgrades only, and the new line rate must be greater than the current line rate.
- The upgrade is accomplished through a series of *sameness policies*.

The sameness policies include the following:

- – The circuit pack must be replaced in the same slot.
- – The upgraded port must retain the same port address.
- – The number of PTPs must remain the same. If the number of PTPs do not remain the same, the database synchronization that occurs after the upgrade will remove the excess number of PTPs; or, if the new circuit pack has more PTPs than the old circuit pack, the database synchronization will add these extra ports.
- – The PM parameters and the history alarms on the port must kept the same before and after the upgrade. (The user must realize that it previously was a lower line speed.)
- – The user must keep the protection group name the same.

- For PTPs, the tool updates the rate only. Other port parameters are updated automatically through the database synchronization that occurs after the upgrade.
- The user must reconcile the cross connections on the NE.
- Other changes in the network topology do not occur during the upgrade process. For example: nodes cannot be added to the topological link during the upgrade process.
- The tool only supports upgrading a topological link in the managed plane. The tool only supports upgrading a TL that does not have optical connections as servers. The topological link to be upgraded should include the topological link through database synchronization process.

TDM NE Optical Lines Upgrade tool log files

The TDM NE Optical Lines Upgrade tool creates an error log file and an activity log file in the following directory:

/var/opt/lucent/logs/oms/tools/optical-lines-upgrade

The names of the log files includes the date and time of the creation.

Examples:

/var/opt/lucent/logs/oms/tools/errorLog.year.month.day.hour.min.sec

/var/opt/lucent/logs/oms/tools//activityLog.year.month.day.hour.min.sec

TDM NE Optical Lines Upgrade tool execution

The TDM NE Optical Lines Upgrade tool can be executed when the management system is up and running. The tool is executed on the HP® server on which the management system is running.

The tool can be manually executed on demand from the command-line. It cannot be scheduled to run as a cron job. To execute the tool on demand from the command line, see the “Run the TDM NE Optical Lines Upgrade Tool from the Command Line” (p. 28-5) task.

Prepare to Run the TDM NE Optical Lines Upgrade Tool from the Command Line

When to use

Use this task to prepare to the TDM NE Optical Lines Upgrade tool from the command line.

Related information

See the following topic in this document:

- "TDM NE Optical Lines Upgrade Concepts" (p. 28-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to prepare to run the NE In-Service Upgrade tool from the command line.

1 Complete the steps in the "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) task to perform a database backup of the management system.

2 Using the documentation that has been provided with the particular NE, execute an NE database backup.

3 Disable the OMS-to-NE connection on the NE to be upgraded.

4 Using the documentation that has been provided with the particular NE, perform the upgrade on the NE. Include all necessary re-routing to ensure a successfully in-service upgrade.

5 Go to the "Run the TDM NE Optical Lines Upgrade Tool from the Command Line" (p. 28-5) task and complete all steps in this task.

END OF STEPS

Run the TDM NE Optical Lines Upgrade Tool from the Command Line

When to use

Use this task to run the TDM NE Optical Lines Upgrade tool from the command line.

Related information

See the following topic in this document:

- "TDM NE Optical Lines Upgrade Concepts" (p. 28-1)
- "Prepare to Run the TDM NE Optical Lines Upgrade Tool from the Command Line" (p. 28-4)

Before you begin

Step 1 of this task requires you to complete the "Prepare to Run the TDM NE Optical Lines Upgrade Tool from the Command Line" (p. 28-4) task.

This tool does not require you to bring the management system down (stop the application).

This tool requires you to know the name of the NE and circuit pack and the slot number of the circuit pack that is to be upgraded.

Task

Complete the following steps to run the NE In-Service Upgrade tool from the command line.

1 Complete all steps in the "Prepare to Run the TDM NE Optical Lines Upgrade Tool from the Command Line" (p. 28-4) task.

2 From the machine on which the management system is running, log in as **oms**.

Result: You are now logged in as **oms**.

3 Enter the following command to execute the NE In-Service Upgrade tool for every upgraded topological link:

```
TDMOpticalLinesUpgrade <A/Z NE Name> <A/Z Circuit Pack Name> <A/
Z Port IDs> <new TL rate>
```

Important! If the topological link to be upgraded is a 1+1 or 1x1 MSP, you can enter only one pair of the A/Z information. The management system locates the other pair (for either the service connection or the protection connection) and upgrade both topological links.

Result: The tool upgrades all connection related configuration information based on the new/higher optical line rate.

END OF STEPS

29 CMISE NE Database Conversion

Overview

Purpose

This chapter explains the concepts and provides the task that is needed to perform a CMISE NE database conversion.

Contents

CMISE NE Database Conversion Concepts

CMISE NE Database Conversion functional description

The CMISE NE Database Conversion process is used to manipulate the image of the Management Information Base (MIB) on a CMISE NE with the intent of downloading that image back to a CMISE NE. The tool is used in the following cases:

- To upgrade a CMISE NE that is currently being managed by a OMS release from NE version RX to RX'; where: the OMS release manages both the X and the X' releases of the NE.
- To perform an NE specific MIB conversion in which the user makes specific modifications to the NE MIB to support special operations in the network.
  Example:
  The process can be used to perform an NE specific MIB conversion if a hardware failure occurs on an NE.
  Specifically, if a CMB406 fails on a 1643 Access Multiplexer (AM) or 1643 Access Multiplexer Small (AMS) NE and it is replaced with a CMB410, the process can be used to upgrade the item code of the main board in the NEs MIB image in the management system database so it can be downloaded to the new NE hardware.

CMISE NE Database Conversion supported platforms

The CMISE NE Database Conversion process is supported on the *Server Platforms*. The CMISE NE Database Conversion process is also supported on the *PC Platform*.

CMISE NE Database Conversion licensing

The CMISE NE Database Conversion process is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the command lines.

CMISE NE Database Conversion upgrade considerations

To perform an upgrade of a CMISE NE, the following considerations must be taken into account:

- The new version of the NE software must be downloaded.
- A new version of the NE database (MIB) must be generated from the old release version. For CMISE NEs, the manager must generate the new database by processing the old version.

CMISE NE Database Conversion and ASAP considerations

OMS enables specific alarm severity assignment profiles (ASAPs) to be assigned to ports during the connection creation process. The NE contains a number of OMS ASAPs; and, when a MIB conversion is performed to or through the first release that supports ASAPs, the NE database conversion adds the standard OMS ASAPs to the NE database.

The following NE releases are considered *the first ASAP supporting releases*:

- 1663 Add Drop Multiplexer (ADMu) R5.2
- 1643 Access Multiplexer (AM)/1643 Access Multiplexer Small (AMS) R7.2
- 1645 Access Multiplexer Compact (AMC) R8.0, R9.0.
- 1655 Access Multiplexer Universal (AMU) R4.1

When performing a MIB conversion that changes the NE release to be one of the releases listed, the management system performs the upgrade and adds the OMS standard ASAPs.

CMISE NE Database Conversion MIB conversion considerations

The following CMISE NE Database Conversions are supported:

- For the 1655 Access Multiplexer Universal (AMU), an upgrade from the ASC101 controller pack to the ASC110 controller pack is supported.
  During the upgrade of the SDH interfaces on an 1655 Access Multiplexer Universal (AMU) from STM-4 to STM-16, a new MIB image must be generated for the 1655 Access Multiplexer Universal (AMU) that changes the line slots from being assigned as ASC101 to being assigned as ASC110.

Configuration instances exist in which the controller pack cannot be changed from the ASC101 to the ASC110. The tool fails when the following invalid configurations are discovered:

- If the pack in TS1 is an ASC108, the VC4#9 or VC#10 is TUG structured and contains TU3s.
- If the SFP in port 1 or 2 has a rate of STM-1.

- For the 1643 Access Multiplexer (AM) and/or 1643 Access Multiplexer Small (AMS), the replacement of the main pack is supported.
  When the main pack in an 1643 Access Multiplexer (AM) and/or 1643 Access Multiplexer Small (AMS) fails and must be replaced, in all probability, an exact match for the original hardware will not be found.
  For instance, the CMB410 or the CMB411 is substituted for the CMB406 because the CMB406 is discontinued. To remedy the ensuing problems caused by this discontinuous and subsequent substitution, OMS provides a tool that can be used to upgrade the main board item code in the NE MIB image in the management system database so it can be downloaded to the new NE hardware.

CMISE NE Database Conversion command line

The following command line is used to execute the CMISE NE Database Conversion:

```
CNA_mib_transform \ -f <pre_upgrade_backup> \ -g <upgrade_mib> \ -n
<ne_to_upgrade> \ -r <transformation name>
```

Where:

<pre_upgrade_backup> is the name of a file to be used to store a copy of the old NE memory file during the conversion process. This file does not get deleted after the tool has completed running in case it is needed to restore the NE database after any failure.

upgrade_mib is the name of a file used to store the new release NE memory after the transformation is complete.

<ne_to_upgrade> is the name of the NE to be upgraded.

<transformation name> is the name of the transformation to perform, see the list of available transformations within the table "Supported upgrade paths" (p. 29-4).

When choosing names for the files to hold the MIB information, the following convention is recommended for the file names:

```
<pre_upgrade_backup>:/tmp/"<NEName>_bak.mib"
```

```
<upgraded_mib>:/tmp/"<NEName>_upg.mib"
```

Important! To accommodate NE filenames that contain characters from the extended character sets, we suggest that you put the filename in quotation marks.

For a list of available transformations, refer to "Supported upgrade paths" (p. 29-4)

Supported upgrade paths

The following table lists the transformation/upgrade paths that are available

NE Type	Old Release	New Release	Transformation Name
1663 Add Drop Multiplexer (ADMu)	R4.0	R5.0	Metro-Universal-R4.0toR5.0
1663 Add Drop Multiplexer (ADMu)	R4.0	R5.1	Metro-Universal-R4.0toR5.1
1663 Add Drop Multiplexer (ADMu)	R5.0	R5.1	Metro-Universal-R5.0toR5.1
1643 Access Multiplexer (AM) and/or 1643 Access Multiplexer Small (AMS)	R5.0	R6.1	Metro-AM/AMS-R5.0toR6.X
1643 Access Multiplexer (AM) and/or 1643 Access Multiplexer Small (AMS)	R5.0	R7.1	Metro-AM/AMS-R5.0toR7.1
1643 Access Multiplexer (AM) and/or 1643 Access Multiplexer Small (AMS)	R6.1	R7.2	Metro-AM/AMS-R6.XtoR7.2
1655 Access Multiplexer Universal (AMU)	R2.0	R3.0	Metro-AMU-R2.0toR3.0
1655 Access Multiplexer Universal (AMU)	R2.0	R4.0	Metro-AMU-R2.0toR4.0
1655 Access Multiplexer Universal (AMU)	R3.0	R4.0	Metro-AMU-R3.0toR4.0
1655 Access Multiplexer Universal (AMU)	R2.1	R4.1	Metro-AMU-R2.1toR4.1
WaveStar® ADM 16/1	R6.2	R7.0	ADM16/1-Senior-R6.XtoR7.0

NE Type	Old Release	New Release	Transformation Name
WaveStar® ADM 16/1	R6.2	R8.0	ADM16/1-Senior-R6.XtoR8.0
WaveStar® ADM 16/1	R7.0	R8.0	ADM16/1-Senior-R7.0toR8.0
1645 Access Multiplexer Compact (AMC)	R8.0	R9.0	AMC R8.0toR9.0

Upgrade CMISE NEs

When to use

Use this task to upgrade a CMISE NE.

Refer OMS Network Element Management Guide for details on the upgrade of CMISE NE via the GUI.

Related information

See the following topic in this document:

- "CMISE NE Database Conversion Concepts" (p. 29-1)

Before you begin

Be aware of and resolve any network issues related to the limitations listed in "Supported upgrade paths" (p. 29-4).

Step 1 of this task can be completed prior to the remaining steps in this task. Step 7 and Step 8

must be done in immediate succession; meaning, you must do Step 8 right after you do step Step 7.

Have the following available:

- The NE software load for the new NE release
- A copy of the *OMS Network Element Management Guide*; this task requires you to use procedures that are documented in this guide, so you must have it handy.
- A copy of the NE Software Release Description for the NE to be upgraded

Task

Complete the following steps to upgrade a CMISE NE.

1 From the management system GUI, download the new software release for the NE (the NE generic) to the NE.

Use the *Download an NE Generic from the Management System to an NE* task that is documented in the *OMS Network Element Management Guide*.

Note that this step can be completed prior to the remaining steps in this task.

2 From the management system GUI, perform an NE database backup for the NE to be upgraded. Note that this backup is to be used if an NE database recovery is required.

Use the *Backup NE Database Versions onto the Management System* task that is documented in the *OMS Network Element Management Guide*.

3 From the management system GUI, de-activate the communications connection with the NE. Use the *Deactivate an OMS-to-NE Connection* task that is documented in the *OMS Network Element Management Guide*.

4 Log in as the **cna** user to the CNA UNIX® server that is connected to the NE to be upgraded.

1. To determine the CNA server, find the Network Communication Group (NCG) for that NE from the **OMS to NE Connections** page on the management system GUI. Use the *Deactivate an OMS-to-NE Connection* task that is documented in the *OMS Network Element Management Guide*.
2. To determine the CNA server, check the Active Network Adapter for this NCG on the Network Communications Group page on the management system GUI.
   Use the *View a List of Network Communications Groups* task that is documented in the *OMS Network Element Management Guide*.

5 From the command line of the CNA UNIX® server, enter the following command line to convert the current memory of the NE to a file that contains the NE memory for the later release of the NE:

```
CNA_mib_transform -f <pre_upgrade_backup> -g <upgrade_mib> -n
<ne_to_upgrade> -r <transformation>
```

Refer to“CMISE NE Database Conversion command line” (p. 29-3) for a description of the parameters that appear in this command line.

6 From the management system GUI, activate the connection with the NE and allow the management system to re-associate with the NE.

Use the *Activate an OMS to NE Connection* task that is documented in the *OMS Network Element Management Guide*.

7 From the management system GUI, perform an **Activate: MIB Clear** on the inactive partition of the NE to be upgraded to enable the NE to run the new release software load.

Use the *Activate an NE Generic on an NE* task that is documented in the *OMS Network Element Management Guide*.

Important! Step 8 must be performed immediately after this step.

8 From the management system GUI, deactivate the connection to the NE to be upgraded.

Use the *Deactivate an OMS to NE Connection* task that is documented in the *OMS Network Element Management Guide*.

9 From the command line of the CNA UNIX® server, enter the following command line to copy the transformed NE memory file from the previous step into the management system database:

```
CNA_restore_nes -f <upgraded_mib>
```

Where:

<upgraded_mib> is the name of the file that contains the new MIB after it has been transformed to the version for the new release, which was generated by the **CNA_mib_transform** in the previous step.

Example:

Using the recommended filenames names in the previous step:

```
CNA_restore_nes -f /tmp/"<NEName>_upg.mib"
```

10 Perform any supported changes to the NE that are required, for example:

- For the 1643 Access Multiplexer (AM) and/or the 1643 Access Multiplexer Small (AMS), replace the main NE pack with the new one. Refer to "CMISE NE Database Conversion MIB conversion considerations" (p. 29-2) for details.
- For the 1655 Access Multiplexer Universal (AMU) ASC101 to ASC110 conversion, replace the existing controller pack with the new controller pack. Refer to "CMISE NE Database Conversion MIB conversion considerations" (p. 29-2) for details.

11 From the management system GUI, activate the connection with the NE and allow the management system to re-associate with the NE. The management system automatically synchronizes its database with the NEs..

Use the *Activate an OMS to NE Connection* task that is documented in the *OMS Network Element Management Guide*.

12 From the management system GUI, retrieve the synchronization information following the re-association in order to verify that the management system has performed a full synchronization.

Refer to the *OMS Network Element Management Guide* for details.

END OF STEPS

30 DMX/DMXtend NE Upgrade

Overview

Purpose

This chapter explains the concepts and provides the task that is needed to perform a migration of NE related data in OMS after certain DMX or DMXtend NE Upgrades are completed.

For DMX NE type, this task is only required when a DMX NE with release earlier than R6.0 is upgraded to a release of R6.0 or higher.

For DMXtend NE type, this task is only required when a DMXtend NE with release earlier than R4.0 is upgraded to a release of R4.0 or higher.

For all other NE Upgrades for DMX and DMXtend NE types, this task is not required.

Contents

DMX/DMXtend NE Upgrade tool overview

Upgrading pre-DMX R6.0/pre-DMXtend R4.0 Network Elements to DMX R6.0/DMXtend R4.0 and higher releases

In DMX R6.0 and later/ DMXtend R4.0 and later, the format for the port names are changed from earlier releases. The information for ports and connections already stored in the OMS database needs to be updated to reflect the new naming. These upgrade tools will accomplish that renaming.

When the software on a DMX NE is upgraded from a release earlier to R6.0 to release 6.0 or higher and when communications are reestablished between OMS and the Network Element, OMS recognizes the version change and will automatically "Deactivate" the NE. The user must upgrade the TNA database for the NE by running an offline tool, upgrade the OMS database by running a second offline tool and then once the upgrades are successfully complete, the user must manually "Activate" the NE and initiate a full DB Synchronization for the Network Element.

When the software on a DMXtend NE is upgraded from a release earlier to R4.0 to release 4.0 or higher and when communications are reestablished between OMS and the Network Element, OMS recognizes the version change and will automatically "Deactivate" the NE. The user must upgrade the TNA database for the NE by running an offline tool, upgrade the OMS database by running a second offline tool and then once the upgrades are successfully complete, the user must manually "Activate" the NE and initiate a full DB Synchronization for the Network Element.

Upgrade DMX/ DMXtend NEs

When to use

Use this task to migrate NE related data in OMS after an upgrade of a DMX/DMXtend NE from a release earlier than R6.0/R4.0 to a release of R6.0/R4.0 or higher is successfully completed.

Related information

See the following topic in this document:

- "DMX/DMXtend NE Upgrade tool overview" (p. 30-2)

Before you begin

Ensure the old release of the DMX/DMXtend NE is up and running from OMS GUI. Before running the upgrade scripts, take a backup of the old database so that it can be recovered if something goes wrong.

Task

Complete the following steps to upgrade a DMX/DMXtend NE.

1 Upgrade the software on the DMX/DMXtend NE. The NE will be upgraded to the later release and the NE will get deactivated in OMS.

Result: OMS will recognize the version change and will automatically "Deactivate" the NE.

2 From the machine on which the management system is running, log in as **`tna`**.

Result: You are now logged in as **`tna`**.

3 Upgrade the TNA database for the NE by running the script:
/opt/lucent/upgrade/bin/upgrade_DMX_TNA_DB <NEName>

Verify the following log file to ensure there are no errors:
/var/opt/lucent/logs/dmx_upgrade_tna_db.log

4 From the machine on which the management system is running, log in as **`oms`**.

Result: You are now logged in as `oms`.

5 Upgrade the OMS database for the NE by running the script:
/opt/lucent/upgrade/bin/upgrade_DMX_OMS_DB <NEName>

Verify the following log file to ensure there are no errors:
/var/opt/lucent/logs/dmx_upgrade_oms_db.log

6 The OMS database is upgraded to support the new NE release. Now proceed with the following:

- Manually activate the NE from OMS
- Initiate a full Database Synchronization Refer to the *OMS Network Element Management Guide* for details on how to Activate an NE and perform a database synchronization.

END OF STEPS

31 NE Name Change

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run NE Name Change command-line tool.

Contents

NE Name Change Concepts

NE Name Change tool definition

The NE Name Change tool enables users to rename the existing names that have been given to network elements (NEs). The NE to be renamed can be a managed network element, a non-managed, or an unknown network element.

Changes to NE names occur must frequently because of the following scenarios:

- Network growth necessitates name changes.
- Operator methods or procedures change.
- An operator error occurs.

This infrequent operation also requires a similar procedure in the NE itself.

NE Name Change tool supported platforms

The NE Name Change tool is supported on the *Server Platforms*. The NE Name Change tool is also supported on the *PC Platform*.

NE Name Change tool licensing

The NE Name Change tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

NE Name Change parameter options

The NE Name Change tool is executed as a simple command-line tool.

The following parameters options can be specified during the execution of the tool:

- **-o** specifies the appropriate old NE names.
- **-n** specifies the appropriate new NE names.
- **-f** specifies the appropriate filename with the full directory path if multiple NE names are to be changed.
- **-c <yes/no>** specifies whether to change the circuit ID in M1400/Telcordia format so the corresponding connection names also reflect the new central office name. If **yes** is specified, the tool replaces the existing central office names in the connection names that are in M1400 or Telcordia format. A connection name in free format is not updated even if the existing NE name in the user input is contained in the connection name string. The default is **no**.

The **-f** option specifies the name of the flat file that contains multiple NE filenames. The format for this input file is as follows:

- The first line of the file is an optional commented line (with a # prefix) that contains a statement such as
  `#Input file for NE name change tool for multiple NEs`.
- Every line after the first line contains the old NE names and the new NE names separated by a **tab** character. Only one old NE name and one new NE name can be entered on each line. The NE names are case sensitive. A maximum of 10 lines containing old NE names and new NE names can be entered.
  Note: Users can swap two NE names in the input file. The new NE names are to indicate such swaps. To support swapping, users should use a temporary NE name in the input file that is not in the management system database.

For example, where the tab character is shown as the ^ symbol:

```
#Input file for NE name change tool for multiple NEs

Alpha1 ^ Alpha1A

Beta1 ^ Beta1A

Gamma1 ^ Gamma1A
```

NE Name Change functional assumptions

The functionality of the NE Name Change tool assumes the following:

- The NE Name Change tool does not change the NE name change at the NE. This change must be performed from CIT; or for TL1 NEs, this change must be performed through the Command Center pages of the management system.
- The IP address or the Network Service Access Point (NSAP) address of the NE is not changed.
- An NE upgrade cannot occur while the NE name is being changed.
- The NE does not clear all standing alarms when the NE name is changed.
- If the NE is a member of a Bidirectional Line Switched Ring (BLSR) or a Multiplex Section - Shared Protection Ring (MS-SPRing) ring, the squelch map is updated only if the automatic squelch map calculation is enabled in the NE; otherwise, the user must update the squelch map data in each NE in the ring.
- All performance monitoring (PM) data stored in the NE is lost. The PM data collected during the execution of the tool is also lost.
- The NE communication to the management system is down for directly managed NEs and the communication of the NE with ITM-SC or EMS is down for indirectly managed NEs.
- The execution of the NE Name Change tool does not trigger any notification to northbound systems.
- Historic data (such as that contained in the Alarm Log, in PM data, or in the User Activity Log) that contains the previous NE name cannot be accessed using the old NE name from the GUI after the tool successfully changes the NE name.
- The execution of the NE Name Change tool does not impact the Data Extraction tool.
- For distributed architecture configurations (CNAs, TNAs, BPM, or GWSs), the NE Name Change tool runs in the management system and triggers the tool that is resident in those distributed applications.
- For NE name (TID) changes for indirectly managed NEs, the appropriate EMS or ITM-SC application should be brought down to run the tool in the respective EMSs. The application should then be brought up after the NE name change at the NE; but, the communication to the NE should still be down. The tool cannot bring down those management systems.
- The tool updates all current data in the OMS database that references the existing NE name with the user entered new NE name, which includes the tables such as Element Administration (EA), network adapters (TNA/CNA), aggregates, areas, geographic domains, connection records (both pending and in-effect) for digital links, connections and Ethernet services, link connection tables, the Alarm List (but not the Alarm Log), network control groups, BLSR/MSSPRING node IDs, performance

measurements, BPM tables, scheduler data, snc and snc component tables.
The new NE names are not be updated in the Alarm Log, Command and Response Log, NE Notification Log, User Activity Log, or in PM history data.
The tool does not update the area names, aggregate names, or the domain names if the existing NE names entered by the user are also assigned to these object.

- For each new NE name in the user input, the tool verifies if a central office name with the partial string of NE name (as per rules of central office name generation) exists in management system database. If a central office name does not exist, a new central office name is created and is entered in the database. If the old central office name exists in the management system database, the tool does not delete the old name.

NE Name Change log files

The NE Name Change tool creates the following log files:

- an activity log file
- a processed log file
- an error log file

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/ne_name_change

The names of the log files include the date and the time of their creation. For example:

errorLog.yyyy.mm.dd.hh.mm.ss

activityLog.yyyy.mm.dd.hh.mm.ss

processedNEnameChageLogLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

The Activity Log contains the following lines:

- The first line of the log file contains the starting date and time.
  Example:
  ```
  NE Name Change tool execution started on 2005, August 2,
  15:30:21
  ```
- The second line of the log file contains the completion date and time.
  Example:
  ```
  NE Name Change tool execution completed on 2005, August 2,
  15:35:13
  ```

The Process log file contains the details of the successfully completed steps in the script, such as

```
NE name change completed successfully in EA, "NE Name change
completed successfully in TNA/CNA.".
```

The Error log contains records from the input file that failed during validation or implementation. The error message that is displayed shows the first record that the system encountered and that caused it to stopped processing.

Prepare to Run the NE Name Change Command-Line Tool

When to use

Use this task to prepare to run the NE Name Change command-line tool.

Related information

See the following topic in this document:

- "NE Name Change Concepts" (p. 31-1)

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to prepare to run the NE Name Change command-line tool.

1 Execute a hot backups on the previous night in case the tool fails to update all of the servers.

2 Verify that any database synchronizations (dbsyncs) or NE backups are not running or are in the queue for the targeted NEs.

3 If you plan to run the tool with the management system application up, stop communication to the directly managed NEs whose names have to be changed using the tool.

For indirectly managed NEs, stop communication to the targeted NEs from the respective element management systems (ITM-SC or EMS).

4 For indirectly managed NEs, stop the communication of the respective ITM-SC or EMS with the management system.

Perform the necessary NE name change procedure on the NE.

Stop the communication to the NE from ITM-SC/EMS.

Restart the communication of ITM-SC/EMS to the management system.

If ITM-SC is in redundant configuration (geographic redundancy), the NE name change should occur in both the primary and secondary ITM-SCs. During this operation, we recommended that you disable the GR switch to avoid any unexpected system behavior.

5 For directly managed NEs, use the NE CIT to change the NE names at the network elements. This task can also be performed from the OMS Command Center for directly managed TL1 NEs before step 1.

Important! This step is not part of the NE Name Change tool.

6 If the NE name change tool is to change more than one NE name, create a flat file with up to 10 entries and load the file in OMS in the appropriate directory.

7 Complete all of the steps in the "Run the NE Name Change Command-Line Tool" (p. 31-8) task.

END OF STEPS

Run the NE Name Change Command-Line Tool

When to use

Use this task to run the NE Name Change command-line tool.

Related information

See the following topic in this document:

- "NE Name Change Concepts" (p. 31-1)

Before you begin

The NE Name Change tool can be run with the management system application up or down according to the following requirements:

- For compact servers, the tool can be run with management system application down and the database up.
- For medium and large servers, the tool can be run with the application up or down.
- If the tool is run with the application up, only users with **oms** permissions can execute the NE Name Change tool.
- If the tool is run with the application down, users with **oms**, **tna**, **cna**, or **bpm** permissions can execute the NE Name Change tool.
  Important! When executing the tool with the management system application down, the CORBA GateWay is also be down; therefore, the administrator must log into each of the following servers and execute the tool: OMS, TNA, CNA, and BPM.
- If the tool is run with application up, the administrator who is executing the tool must notify (possibly via email) all active users to refresh their screens.

Step 1 of this task requires you to complete the "Prepare to Run the NE Name Change Command-Line Tool" (p. 31-6) task.

The last step in this task requires you to continue with the "Post Processing After Running the NE Name Change Command-Line Tool" (p. 31-10) task.

While the tool is processing the input file for multiple NEs, you can terminate its execution by entering CTRL C. Entering CTRL C terminates the execution of the tool after the current running process. The termination of the tool is logged in the Activity Log.

Task

Complete the following steps to run the NE Name Change command-line tool.

1 Complete all of the steps in the "Prepare to Run the NE Name Change Command-Line Tool" (p. 31-6) task.

2 If you are executing this tool with the management system up, log in as **oms** from the machine on which the management system is running

If you are executing this tool with the management system down, log in once to each of the following servers and execute the tool on that server: **oms**, **tna**, **cna**, and **bpm**.

3 Enter the following command line to invoke the NE Name Change command line tool:

```
ne_name_change -o <old NE Name> -n <new NE name> -f <filename &
full path> -c <yes/no>
```

Result: If the tool completes successfully, it updates the referenced data in the management system. If the tool was run with the management system application up, it re-establishes communication for all directly managed NEs in the flat file that contains the list of old NE names and new NE names and it updates the network map accordingly. If the tool was run with the management system application down, it re-establishes communication with all directly managed NEs when the application is brought back up. Go to Step 5.

If the tool fails, it prompts you for direction regarding the disposition of its status file. Go to step Step 4.

4 If the tool fails, it asks if you want to want to rerun the tool using the old status file, which contains pertinent information from the previous execution of the tool. If you want to rerun the tool using the old status file, answer **yes**. The tool continues its execution.

If you do not want to rerun the tool using the old status file, answer **no**. The tool then asks if you want to remove the old status file. Answer **yes** or **no**.

5 Once the tool has successfully executed, complete all the steps in the "Post Processing After Running the NE Name Change Command-Line Tool" (p. 31-10) task.

END OF STEPS

Post Processing After Running the NE Name Change Command-Line Tool

When to use

Use this task to perform the needed post processing steps that must be completed after the NE Name Change command-line tool is run.

Related information

See the following topic in this document:

- “NE Name Change Concepts” (p. 31-1)
- “Prepare to Run the NE Name Change Command-Line Tool” (p. 31-6) task
- “Run the NE Name Change Command-Line Tool” (p. 31-8) tass

Before you begin

Step 1 in this task requires you to complete the “Prepare to Run the NE Name Change Command-Line Tool” (p. 31-6) and “Run the NE Name Change Command-Line Tool” (p. 31-8) tasks.

Task

Complete the following steps to perform the needed post processing steps that must be completed after the NE Name Change command-line tool is run.

1 Complete all of the steps in the “Prepare to Run the NE Name Change Command-Line Tool” (p. 31-6) and “Run the NE Name Change Command-Line Tool” (p. 31-8) tasks.

2 Check the log files for errors and fix any errors that might have occurred.

3 If needed, shut down and restart the GUI Web Server to update the cache memory.

4 Perform a database synchronization (dbsync) to resynchronize the respective NEs for alarms.

5 If applicable, restart PM collection on the NEs.

END OF STEPS

32 NE Reparenting

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run NE Reparenting.

NE Reparenting enables users to reparent, or to *move*, one or more of the following:

- CMISE network elements (NEs) from an ITM-SC R11.4.3 managed network to a CMISE network adapter (CNA) managed network via a command-line tool
- CMISE NEs from a CMISE network adapter (CNA) to CMISE network adapter (CNA) via a set of tasks that includes command and GUI operations
- TL1 NEs from a TL1 network adapter (TNA) to TL1 network adapter (TNA) via a set of tasks that includes command and GUI operations
- 1671 Service Connect (SC) NEs from a Network Management Adapter (NMA) to a Network Management Adapter (NMA) via a set of tasks that includes command and GUI operations

Contents

NE Reparenting Concepts for ITM-SC R11.4.3 NEs

NE Reparenting tool for ITM-SC R11.4.3 NEs definition

The NE Reparenting command line tool for ITM-SC R11.4.3 NEs enables users to reparent, or to *move*, one or more CMISE network elements (NEs) from an ITM-SC R11.4.3 managed network to a CMISE network adapter (CNA) managed network. The use of this tool enables OMS customers, who are migrating from Navis® NMS to OMS, to continue to manage their existing CMISE NEs under ITM-SC until they are ready to move to a CNA.

NE Reparenting for ITM-SC R11.4.3 NEs supported platforms

The NE Reparenting tool is supported on the *Server Platforms*. The NE Reparenting tool is also supported on the *PC Platform*.

NE Reparenting for ITM-SC R11.4.3 NEs licensing

The NE Reparenting tool for ITM-SC R11.4.3 NEs is part of the “OMS_CORE license” (p. 5-5). A separate license is not needed to execute the tool.

NE Reparenting for ITM-SC R11.4.3 NEs tool functionality

Through a set of screens of interactive screens, the NE Reparenting tool for ITM-SC R11.4.3 NEs enables users to specify up to 10 NEs to be moved to an appropriate CMISE network adapter (CNA) and Network Communications Group (NCG). The NE Reparenting tool can also be executed by specifying an input filename when reparenting more than 10 NEs. The tool moves the specified NEs to the CNAs and NCGs, along with the following data in Element Administration (EA) tables:

- Network Communication Group (NCG) type (OSI for CMISE NEs)
- NE Type
- NE Release
- Network Service Access Point (NSAP) address
- Communication status

The tool then updates all internal references in the management system database and enables Bulk Performance Monitoring (BPM) to start data collection.

NE Reparenting for ITM-SC R11.4.3 NEs non-supported scenarios

The NE Reparenting tool does not support the following scenarios:

- The NE Reparenting tool does not support the scenario of reparenting a CNA/TNA to ITM-SC/EMS, which is reparenting in the reverse direction.
- The NE Reparenting tool does not support the scenario of reparenting an NE from one ITM-SC to another ITM-SC or from one EMS to another EMS. An NE can be reparented from one ITM-SC to another ITM-SC or from one EMS to another EMS only through notifications from the NE.
- The deletion of an NE in ITM-SC/EMS and creation of an NE in another ITM-SC/EMS in a reparenting scenario is done from the respective ITM-SC/EMS GUIs.

NE Reparenting for ITM-SC R11.4.3 NEs functional requirements

The NE Reparenting tool adheres to the following functional requirements:

- The NE Reparenting tool can be run from the command line of any monitor that is connected to the HP® server.
- The NE Reparenting tool can be executed while the OMS application is up and running.
- Optionally, communication to appropriate ITM-SC can be brought down until the reparenting is completed; however, it is not a requirement. Provisioning activities are not allowed on the NE while the NE is being reparented.
- Only users with **oms** permissions can execute the NE Reparenting tool.
- The NE release under ITM-SC or its TID is not changed during reparenting.
- An alarm synchronization for the NE from the new (reparented) ITM-SC/EMS must be performed after the reparenting in order to update alarm IDs and to preserve alarm acknowledgement data. If a **clear** is received after the NE is reparented, the corresponding alarm record is cleared in the management system.
- The association between ITM-SC and the NE must be disabled before the NE Reparenting tool is executed on the particular NEs.
- The **.rhost** files must be set up to enable **rsh**, providing that the files were not already set up for MigrationMaster.

NE Reparenting for ITM-SC R11.4.3 NEs input file format

The NE Reparenting tool offers users the option of creating an input file that consists of a list of NE names, one on each separate line, that are to be reparented. The file can contain an unlimited number of NEs. This input file, along with its full directory path, can be specified when the NE Reparenting tool is executed with the **-f** option.

Optionally and for ease of use, the first line of the input file should be prefaced with the **#** character to indicate a comment. The **#** should be followed by the name of the ITM-SC from which all the NEs are required to be reparented.

To facilitate the running of the tool, you can list the NEs from one ITM-SC into more than one input file. However, only one path and filename can be entered with the when you specify the **-f** option.

NE Reparenting for ITM-SC R11.4.3 NEs log files

The NE Reparenting tool creates the following log files:

- an error log file
- an activity log file, along with a running activity log
- a processed log file

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/ne_reparent

The names of the log files include the date and the time of their creation. For example:

errorLog.yyyy.mm.dd.hh.mm.ss

activityLog.yyyy.mm.dd.hh.mm.ss

processLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

The Activity Log contains the following lines:

- The starting date and time.
  Example:
  ```
  NE Reparenting tool execution started on 2005, August 2,
  15:30:21
  ```
- The result of the execution.
  Example:
  ```
  Five network elements are reparented in this execution.
  ```
- The tool completion date and time.
  Example:
  ```
  NE Reparenting tool execution completed on 2005, August 2,
  15:35:13
  ```

The tool also outputs a Running Activity log that is displayed during execution of the tool. This log contains the same information as the Activity Log. Users are encouraged to terminate the display of the Running Activity Log by entering an **X**, for e**X**it, on its screen.

The Process log file contains the details of the successfully completed steps in the script, such as `NE names validated successfully`.

The Error log contains records from the input file that failed during validation or implementation. The error message that is displayed shows the first record that the system encountered and that caused it to stopped processing.

NE Reparenting Concepts for NA to NA

NE Reparenting for NA to NA definition

The reparenting of a network element (NE) from one Network Adapter (CNA, TNA or NMA) to another Network Adapter enables users to reparent, or to *move*, one CMISE network adapter (CNA) or one TL1 network adapter (TNA) or Network Management Adapter (NMA) to another CNA or TNA or NMA.

Users perform the reparenting by modifying the network communications group (NCG) of the NE using the Modify OMS-NE Connections Page of the management system. Each NE is assigned to one and only one NCG. In turn, each NCG is associated with one and only one NA or controller. So, the modification of the NCG of the NE results in moving the NE to the new NA if the new NCG is associated with a different NA.

In addition, users can move an entire NCG from one NA to another NA, which results in all of the NEs in the NCG being moved from one NA to another.

NE Reparenting for NA to NA supported platforms

The use of NE Reparenting for NA to NA is supported on the *Server Platforms*. The use of NE Reparenting for NA to NA is also supported on the *PC Platform*, for CMISE NEs only.

NE Reparenting for NA to NA licensing

The NE Reparenting is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Run the ITM-SC NE Reparenting Command-Line Tool

When to use

Use this task to run the NE Reparenting command-line tool for ITM-SC R11.4.3 NEs.

Related information

See the following topic in this document:

- "NE Reparenting Concepts for ITM-SC R11.4.3 NEs" (p. 32-2)

Before you begin

The NE Reparenting tool for ITM-SC R11.4.3 NEs can be executed while the OMS application is up and running.

Once the tool is executed, a series of screens appear. Each screen requires your input and each screen concludes with most, if not all, of the following, choices:

- <**P**revious> brings up the previous screen and enables you to make any necessary changes.
- <**N**ext> brings up the following step.
- <e**X**it> terminates the execution of the tool and all of your input from the system.
- <**F**inish> indicates to the system your completion of data and that the tool should complete its execution.

Task

Complete the following steps to run the NE Reparenting command-line tool for ITM-SC R11.4.3 NEs.

1 From ITM-SC screens, stop the communication to all the NEs that are to be reparented.

2 From the machine on which the management system is running, log in as **oms**.

3 Login to ITM-SC as **i2kadmin** user.

Use the **vi** editor to access the **.rhosts** file and add the following entry:

```
<oms ip> oms
```

Save the change that you have made to the file.

4 Enter the following command line to invoke the NE Reparenting command line tool:

```
ne_reparent -f<full directory path including the input file>
```

Result: If you did not enter the full directory path of the input file, the tool outputs a message that instructs you to enter the names of up to 10 NEs that are to be reparented. Go to Step 5.

If you entered the full directory path of the input file, the tool prompts you to for reparent information. Go to step Step 6.

Regardless of your entry, the tool displays a Running Activity Log, which you can exit by entering an **X** (for e**X**it).

5 On separate lines, enter the names of up to 10 NEs that are to be reparented to the same CNA and the same Network Control Group (NCG) and enter **N** for Next, in order to proceed to the next screen.

Result: The tool verifies that the names that you have entered exist in the management system database, that the releases of the NE names entered are reparentable under CNA, and that you have not exceeded 10 entries. If you have violated any of these verifications, the tool outputs an appropriate error message.

If you hvae not violated any of these verifications, the tool outputs a list of available CNAs.

6 Enter the number of the CNAs that you want the NEs to reparent to and enter **N** for Next, in order to proceed to the next screen.

Result: The tool outputs a list of the Network Control Groups (NCGs) that exists for the CNAs that were previously selected.

7 Enter the number of the NCG that you want the NEs to reparent to or enter the name of a new NCG; then, enter **F** for Next, in order to finish the execution.

Results: The tool moves the specified NEs to the appropriate network adapter and Network Control Group, along with the following data in Element Administration (EA) tables:

- Network Communication Group (NCG) type (OSI for CMISE NEs)
- NE Type
- NE Release
- Network Service Access Point (NSAP) address
- Communication status

The tool then updates all internal references in the management system database, enables the BPM to start data collection, and prompts you to shutdown and restart the GUI web server (GWS).

8 Use the "Stop the Platform" (p. 9-7) and "Start the Platform" (p. 9-5) tasks to shutdown and restart the GWS.

9 Perform a database synchronization by NCGs from the pages of the management system. Use the following path:

Tools > Database synchronization

END OF STEPS

Reparent CMISE NEs from a CNA to Another CNA

When to use

Use this task to reparent CMISE NEs of a network communication group from a CMISE network adapter (CNA) to another CNA.

Related information

See the following topic in this document:

- "NE Reparenting Concepts for NA to NA" (p. 32-5)

Before you begin

This task can be executed while the OMS application is up and running.

Task

Complete the following steps to migrate CMISE NEs from a CMISE network adapter (CNA) to another CNA.

1 Identify the network communications group (NCG) with which the CMISE NEs are associated.

2 Using the steps provided in the *OMS Network Element Management Guide*, go to the Modify Network Communications Group (NCG) task and change the NA server name to the name of the target NA server.

Result: The management system automatically transfers the NEs in the modified NCG to an alternate NA server and reconnects to each of the transferred NEs.

3 Perform a database synchronization by NCGs on the pages of the management system:

Tools > Database Synchronization

4 On the server where BPM is running, restart BPM processes using the following command lines:

Log in as **bpm**.

```
platform_cntrl stop
platform_cntrl start
```

END OF STEPS

Reparent TL1 NEs from TNA to Another TNA

When to use

Use this task to reparent TL1 NEs of a network communication group from a TL1 network adapter (TNA) to another TNA.

Related information

See the following topic in this document:

- "NE Reparenting Concepts for NA to NA" (p. 32-5)

Before you begin

This task can be executed while the OMS application is up and running.

Task

Complete the following steps to reparent TL1 NEs from a TL1 network adapter (TNA) to another TNA.

1 Identify the network communications group (NCG) with which the TL1 NEs are associated.

2 On the server with which the NEs originally communicated, enter the following command lines to backup synchronization data from the TNA database for all NEs that are associated with this NCG:

On the server, log in as **tna**

If source TNA is coresident use the following command:

```
migration_tna -export name_of_NCG
```

If source TNA is distributed use the following command:

```
migration_tna_export "nelist"
```

Note: The "nelist" is a list of NEs associated with the NCG and each NE TID/name must be enclosed in double quotes and separated by a space. For example:

```
migration_tna_export "NE-name-1" NE-name-2" NE-name-3"
```

Result: The following tables are exported to **/var/work/migration/tna**: NEINFO, EQUIPMENT, EQUIPATTRIBUTE, NEATTRIBUTE, TP, TPPARAMETERS, TPGROUP, TPMUXGROUPLEG, PROTGROUP, and PROTGROUPPARAMETERS.

3 Using the steps provided in the *OMS Network Element Management Guide*, go to the Modify Network Communications Group (NCG) task and change the NA server name to the name of the target NA server.

Result: The management system automatically transfers the NEs in the modified NCG to an alternate NA server and reconnects to each of the transferred NEs.

4 Use the following command lines to copy the TNA synchronization data from the server with which the NEs originally communicated, to restore the synchronization data, and to update the synchronization status:

On the target server with which the NEs are communicated now, log in as **tna**

```
migration_tna -ftpget
```

The tool prompts you for the following two lines:

```
<IP address of the server with which the NEs originally
communicated>
```

```
<TNA password of the server with which the NEs originally
communicated>
```

When the tool has completed running, enter the following command line:

```
migration_tna -import
```

5 On the server where BPM is running, restart BPM processes using the following command lines:

Log in as **bpm**.

```
platform_cntrl stop
```

```
platform_cntrl start
```

END OF STEPS

Reparent 1671 SC NEs from a NMA to Another NMA

When to use

Use this task to reparent 1671 Service Connect (SC) NEs of a network communication group from a Network Management Adapter (NMA) to another NMA.

Related information

See the following topic in this document:

- "NE Reparenting Concepts for NA to NA" (p. 32-5)

Before you begin

This task can be executed while the OMS application is up and running.

Task

Complete the following steps to migrate 1671 Service Connect (SC) NEs from a Network Management Adapter (NMA) to another NMA.

1 Identify the network communications group (NCG) with which the 1671 Service Connect (SC) NEs are associated.

2 Using the steps provided in the *OMS Network Element Management Guide*, go to the Modify Network Communications Group (NCG) task and change the NA server name to the name of the target NA server.

Result: The management system automatically transfers the NEs in the modified NCG to an alternate NA server and reconnects to each of the transferred NEs.

3 Perform a database synchronization by NCGs on the pages of the management system:

Tools > Database Synchronization

4 On the server where BPM is running, restart BPM processes using the following command lines:

Log in as **bpm**.

```
platform_cntrl stop
platform_cntrl start
```

END OF STEPS

33 EPT Route ID Update

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run EPT Route ID Update command line tool.

Contents

EPT Route ID Update Tool Concepts

EPT Route ID Update tool definition

The EPT Route ID Update Tool is a command line tool that supports the updating of the route ID for in-effect existing and pending LambdaXtreme™ Transport connections in the Network Resource Manager (NRM) and OMS databases using EPT generated Route ID values.

With EPT Route ID Update, 1625 LambdaXtreme® Transport users who are using OMS, EPT, and NRM can manage 1625 LambdaXtreme® Transport connections and can synchronize route ID information in the three databases. Because EPT adds the route ID to in-effect existing or pending routes that already exist in the databases, the execution of this tool should only occur once.

EPT Route ID Update tool supported platforms

The EPT Route ID Update tool is supported on the *Server Platforms*. The EPT Route ID Update tool is not supported on the *PC Platform*. The PC Platform does not support TL1 NEs.

EPT Route ID Update tool licensing

EPT Route ID Update tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

EPT Route ID Update functionality

In conjunction with the EPT Route ID Update tool, performs the following tasks:

- Enables the user to retrieve (via FTP or HTML Browser by a OMS user) a Route ID file (route_ids) from EPT that contains all optical channel connections.
- Identifies the connection name that is associated with each EPT route ID in the management system database.
- Adds the route ID to the management system database if a connection name can be found.
- Adds the connection name to a new processed route ID file. If the connection name cannot be identified, it remains blank in the file.
- Provides an exception report that identifies any In-Effect route ID that cannot be associated with an OMS connection name.
- Stores and allows NRM to retrieve the modified EPT route ID file to be retrieved.

EPT Route ID Update tool functional requirements

The EPT Route ID Update tool adheres to the following functional requirements:

- The 1625 LambdaXtreme® Transport EPT release is Release 2.1, which is capable of assigning route IDs.
- The user has downloaded the OMS data to EPT in order to update the appropriate route database states to **In-Effect**.
- The user has manually updated the route database states for any connections that are in NRM that have not reached **Implementation Complete**; meaning, the connection is not yet in the management system. This requirement can be ignored if only **In-Effect** routes are being updated.
- The Network Resource Management and OMS cannot both create connections that are in each other's database.

EPT Route ID Update log files

The EPT Route ID Update tool creates the following log files:

- an activity log file, along with a running activity log
- an exception report
- a processed log file

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/ept_route_id_update

The names of the log files include the date and the time of their creation. For example:

activityLog.yyyy.mm.dd.hh.mm.ss

exception_route_ids.yyyy.mm.dd.hh.mm.ss

processed_route_ids.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

The Activity Log contains the following lines:

- The starting date and time.
  Example:
  ```
  EPT Route ID Update tool execution started on 2005, August 2,
  15:30:21
  ```
- The result of the execution.
  Example:
  ```
  725 EPT Routes have been processed. 25 EPT In-Effect Routes
  could not be matched with an OMS Connection.
  ```
- The tool completion date and time.
  Example:
  ```
  EPT Route ID Update tool execution completed on 2005, August
  2, 15:35:13
  ```

The tool also outputs a Running Activity log that is displayed during execution of the tool. This log contains the same information as the Activity Log. Users can terminate the display of the Running Activity Log by entering an **X**, for e**X**it, on its screen.

The Exception report contains a list of EPT In-Effect Route IDs that could not be matched with an OMS connection.

The Processed EPT Route ID log contains the original EPT **route_ids** file with the OMS connection name added as the first field in each row or record. If a match does not occur, the connection name is remains blank.

Run the EPT Route ID Update Command-Line Tool

When to use

Use this task to run the EPT Route ID Update command-line tool for 1625 LambdaXtreme® Transport NEs.

Related information

See the following topic in this document:

- "EPT Route ID Update Tool Concepts" (p. 33-1)

Before you begin

The EPT Route ID Update command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the EPT Route ID Update command line tool for 1625 LambdaXtreme® Transport NEs.

1 From the machine on which the management system is running, log in as `oms`.

2 Enter the following command line to change directories:

```
cd /opt/lucent/platform/bin
```

Result: You are now in the **opt/lucent/platform/bin** directory.

3 Enter the following command to verify that you are in the correct directory:

```
pwd
```

Result: The system displays the name of the directory. The directory that is displayed should be **bin**.

4 Using ftp or another copy tool, save the route_ids file to the following location:

```
/var/opt/lucent/logs/oms/tools/ept_route_id_update/route_ids
```

If the **ept_route_id_update** directory does not exist, use the **mkdir** command to create the directory.

For example, you would type the following command line:

```
mkdir ept_route_id_update
```

5 Enter the following command line to invoke the EPT Route ID Update command line tool:

```
ept_route_ID_update
```

Result: The tool outputs an informational screen.

6 Enter **F** for **Finish** to indicate that you have completed your input and you want to continue to run the tool.

Result: The tool outputs a message similar to the following:

```
Checking access permissions... Checking if OMS is running
Overall System status... [running] 6 EPT Routes have been
processed.  6 EPT In-Effect Routes could not be matched w ith
an OMS connection. The tool execution is successfully
completed at Mon May  8 13:22:48 EDT 2006.
```

You can close running activity log screen by entering an **X** (**eXit**).

7 Check the output files, which can be found in the following directory:

```
/var/opt/lucent/logs/oms/tools/ept_route_id/update/<processed_
route_ids...><exception_route_ids...><activityLog...>
```

Result: The tool creates the processed_route_ids, exception_route_ids, and activityLog files.

For example, the file names appear as the following:

```
activityLog.2006.05.08.17.21.13

exception_route_ids.2006.05.08.17.21.13

processed_route_ids.2006.05.08.17.21.13
```

END OF STEPS

34 ONNS

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the command line tools that are associated with the Optical Network Navigator System (ONNS).

Contents

ONNS Overview

ONNS definition and functionality

The Optical Network Navigator System (ONNS) is software and hardware bundle that is present on some NEs. ONNS performs connection management functions for synchronous connections, across a network of switched NEs. ONNS consists of a number of ONNS modules. Each module resides on a different switched NE in the network.

ONNS-related tools

The following command line tools are related to ONNS:

- ONNS Defragmentation tool, which is explained in "ONNS Defragmentation Tool Concepts" (p. 34-2) and the "Run the ONNS Defragmentation Command-Line Tool" (p. 34-7) task.
- Discover ONNS Route tool, which is explained in "Discover ONNS Paths Tool Concepts" (p. 34-3) and "Run the Discover ONNS Paths Tool Manually" (p. 34-9) and "Run the Discover ONNS Paths Tool Automatically" (p. 34-10) and "Run the TDM services move Tool" (p. 34-12) tasks.

ONNS Defragmentation Tool Concepts

ONNS Defragmentation tool definition and functionality

The ONNS Defragmentation is a command line tool that is used to identify connections that have could have been impacted by the defragmentation operation that was previously performed on the NE CIT.

The tool requires users to input the neighbor NEs and ports and a scope, which is defined as the **port**, **emptyport**, or **link** on which the defragmentation was performed. The information that the management system user enters must match the information on what was done on the NE for defragmentation. The tool then marks the ONNS service connections riding on the digital links on these ports or between the NEs as **Stale** to indicate that some changes have occurred in the route of these connections. Users can then view the connections on the Graphical Layout to determine the most up-to-date route.

ONNS Defragmentation tool supported platforms

The ONNS Defragmentation tool is supported on the *Server Platforms*. The ONNS Defragmentation tool is also supported on the *PC Platform*.

ONNS Defragmentation tool licensing

The ONNS Defragmentation tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

ONNS Defragmentation tool functional requirements

The ONNS Defragmentation tool adheres to the following functional requirements:

- The ONNS Defragmentation tool can be invoked from the command line of HP® server on which the management system is running after a successful or an unsuccessful defragmentation operation on the NE craft interface terminal (CIT).
- The list of connections that the ONNS Defragmentation tool marks as **Stale** could be an in-exact list of connections that were impacted by defragmentation operation.

  The **Stale** list could be an in-exact list for the following reasons:

  - If the connections have never been viewed on the Graphical Layout, an association does not exist between the connection and the digital link on which it is riding.
  - Since the management system is not aware of link bundling in ONNS, defragmentation on a link bundle can potentially impact all digital links that ride among the NEs in the management system.
  - If the defragmentation operation fails in ONNS, only some connections could have been moved. Since the management system cannot know which connections were moved and which ones were not, the management system marks all the connections riding on the digital link as **Stale**. So, the ONNS Defragmentation tool could potentially mark more connections as **Stale** compared to the list of connections that were actually moved in ONNS.

Discover ONNS Paths Tool Concepts

Discover ONNS Paths tool definition and functionality

The Discover ONNS Paths command line tool allows the user to periodically retrieve the routes of ONNS connections that are in the *Stale* or *Unknown* states in OMS. The retrieval is done by sending a TL1 command to the network and storing the new route in OMS.

To allow for the automatic retrieval, the user must enable the "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter in OMS. Once the installation parameter is enabled, the route reconciliation occurs periodically based on the user setting the time via the **crontab -e** command (UNIX command). The tool can be also be manually invoked from the command line to synchronize the routes of the Stale or Unknown ONNS connections with those existing in the network.

Discover ONNS Paths tool supported platforms

The Discover ONNS Paths tool is supported on the *Server Platforms*. The Discover ONNS Paths tool is also supported on the *PC Platform*.

Discover ONNS Paths tool requirements

The following requirements apply to the successful execution of the Discover ONNS Paths tool:

- ONNS must be enabled in OMS and the user must be an OMS user.
- The "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter must be set to YES if the tool is to be run periodically.
- The user must use the **crontab -e** command for the periodic discovery of ONNS routes.

Discover ONNS Paths tool location and modes of operation

The Discover ONNS Paths tool is located in the following directory:

/opt/lucent/oms/bin

The Discover ONNS Paths tool can be invoked in one of the following two ways:

- automatically from the command line, in which the "ONNS Paths Auto Retrieval" (p. 6-47) must be set to YES:

  ```
  discoverONNSpaths.oms
  ```
- manually from the command line, in which the "ONNS Paths Auto Retrieval" (p. 6-47) does not have to be set to YES:

  ```
  discoverONNSpaths.oms -m
  ```

Discover ONNS Paths tool logs

The Discover ONNS Paths tool creates the following files:

- The tool writes to a trace file that is called **discoverONNSRoute.trace**.
- The tool stores connections whose routes are retrieved in a separate log file called **retrievepaths.log.invocation time**, in which *invocation time* is the time on the OMS system in which the tool has been invoked.
  Connections whose routes were *Stale* or *Unknown* when the tool was invoked now have **Control Plane Path State** as *Known* and the routes are synchronized with those in the network. The tool applies to Add, Discover and Re-arrange orders.

Tool for moving TDM services from one card (NE) to different card (NE)

TDM services move tool definition and functionality

This OMS tool allows the user to move ONNS traffic, including VCG servers, from one Customer/Client port on an NE to another Customer/Client port on the same or different NE.

The script takes a Customer/Client port on a particular NE as input and creates multiple files (create and delete text files) based on the current snapshot that OMS has of the ONNS network. The OMS user can then modify and save the create text files with the desired NE/port information through the OMSCommand Builder screens. The user can execute the delete text files to delete the existing ONNS connections through the OMSCommand Builder on a per source NE basis. The back end also deletes the resulting improper disconnected connections. To create the new connections, the user must execute the modified create files through the Command Builder on a per source NE basis and OMS will inventory these new connections.

TDM services move tool pre-conditions

In order for the TDM services move tool to function as accurate as possible, the user must:

- Run the Network Connections database synchronization on all the NEs to pick up all the connections from the network that may have been set up from the CIT.
- Run the discover ONNS paths script to discover the route details of any Stale connections.

TDM services move tool functional requirements

The following functional requirements apply to the successful execution of the TDM services move tool:

- The script finds all the In-Effect ONNS connections in OMS that are either originating or terminating on the user input Customer/Client port on an user selected NE. These connections can be of the following order types - Add, Discover or Re-arrange with ASTN protection types of Unprotected, Network 1+1 Protected (RVR, NRV), Permanent 1+1 Protected (RVR, NRV), and Auto Reroute (RVR, NRV).
- OMS creates multiple files in a format readable by the command builder
  - Create network connection text files - with ONNS TL1 create commands of the network connections currently existing in OMS. One file per source NE of the existing connection is created.
  - Create protection group text files - with LU TL1 commands to create RVR protection groups for ASTN protection types of Network and Permanent 1+1 Protected RVR connections. For each RVR connection, two files are created - one for the source NE and one for the destination NE to change the protection group to RVR (from a default of NRV).
  - Delete network connection text files - with ONNS TL1 delete commands of the network connections currently existing in OMS, one file per source NE of the existing connection is created.
- When the user triggers the delete files to delete the connections, OMS will mark the connections as improperly disconnected. The user will have to manually delete these improper disconnected connections. User can then execute the modified create file(s) on the desired source NE(s).

Notes

- The TDM services move tool does not apply to ASTN Y connections and MBYN connections.
- OUCs will not be moved, but when the ONNS connection that has OUC is deleted using this tool, the OUC will not be re-created with the new connection.
- When the VCG servers are all deleted, an empty VCG will exist. Any Ethernet services on this will still remain in OMS.
- The user is expected to manually clean up the Ethernet services and/or the VCG and re-create them after the new connections are provisioned. A separate script exists for this. Refer to the section "Tools for moving Ethernet services from one card to another card " (p. 37-7) for the user flow when the ONNS connections are VCG servers.
- For Network 1+1 Protected and Permanent 1+1 Protected connections, separate files with protection group creation commands will be created.

Run the ONNS Defragmentation Command-Line Tool

When to use

Use this task to run the Optical Network Navigator System (ONNS) Defragmentation command-line tool.

Related information

See the following topic in this document:

- "ONNS Defragmentation Tool Concepts" (p. 34-2)

Before you begin

Step 1 of this task requires you to perform the defragmentation on the NE CIT before executing this command-line tool.

The ONNS Defragmentation command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the ONNS Defragmentation command line tool.

1 Perform the defragmentation on the NE CIT.

2 From the machine on which the management system is running, log in as **oms**.

3 Enter the following command line to invoke the ONNS Defragmentation command line tool:

```
astn_defrag
```

Result: The tool requests you to specify the neighbor NEs and ports and a scope (port, link, emptyport). The info that you enter must match the information that was on the NE for defragmentation.

4 Specify the scope to be **port**, **emptyport**, or **link**.

Result: Depending on your input, the tool requires you to input additional information.

5 If the scope is **port** or **emptyport**, go to step Step 6.

If the scope is **link**, go to step Step 7.

6 If the is scope **port** or **emptyport**, specify the **From NE**, which is an ONNS-enabled 1675 Lambda Unite MultiService Switch (MSS) NE.

Result: The tool searches for network owned digital links of rates OC-3, OC-12, OC-48, and OC-192 and/or STM-1, STM-3, STM-16, and STM-64 that have one end point that matches your entry. In addition, the tool locates all connections with category = controlled plane with rates VC-n/STS-n that are riding on this digital link. (These connections could have originating points on NEs other than those that you have specified.) These connections could be service or infrastructure connections such as VCG servers. If the control plane path state of these connections is **Known**, the tool marks them as **Stale**. If the control plane path state of these connections is already **Stale**, they are marked as **no op**. If the control plane path state of these connections is **Unknown**, the tool does not locate them.

7 If the scope is **link**, specify the **From NE**, which is an ONNS-enabled 1675 Lambda Unite MultiService Switch (MSS) NE and the **To NE**, which is an ONNS-enabled 1675 Lambda Unite MultiService Switch (MSS) NE.

Result: The tool searches for all network owned digital links between the From NEs/To NEs that matches your entry. In addition, the tool locates all connections with category = controlled plane with rates VC-n/STS-n that are riding on this digital link. (These connections could have originating points on NEs other than those that you have specified.) These connections could be service or infrastructure connections such as VCG servers. If the control plane path state of these connections is **Known**, the tool marks them as **Stale**. If the control plane path state of these connections is **Unknown**, the tool does not locate them.

8 Open an instance of the management system and view the connections on the Graphical Layout to determine the most up-to-date route.

END OF STEPS

Run the Discover ONNS Paths Tool Manually

When to use

Use this task to run the Discover ONNS Paths Tool manually.

Related information

See the following topics in this document:

- "Discover ONNS Paths Tool Concepts" (p. 34-3)
- "Run the Discover ONNS Paths Tool Automatically" (p. 34-10) task

Before you begin

Remember that in order to run the tool manually, the "ONNS Paths Auto Retrieval" (p. 6-47) installation must be set to NO.

To run this tool automatically, use the "Run the Discover ONNS Paths Tool Automatically" (p. 34-10) task.

Task

Complete the following steps to run the Discover ONNS Paths Tool manually.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command line to invoke the tool:

```
discoverONNSpaths.oms -m
```

Result: The tool creates two types of log files upon completion. See "Discover ONNS Paths tool logs" (p. 34-4) for details.

END OF STEPS

Run the Discover ONNS Paths Tool Automatically

When to use

Use this task to run the Discover ONNS Paths Tool automatically.

Related information

See the following topics in this document:

- "Discover ONNS Paths Tool Concepts" (p. 34-3)
- "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter
- "Modify an Installation Parameter" (p. 6-167) task
- "Run the Discover ONNS Paths Tool Manually" (p. 34-9) task

Before you begin

Before you run the tool automatically, the **crontab -e** UNIX command must be run.

In addition, to run the tool automatically, the "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter must be set to **YES**. You will be setting this installation parameter to YES in Step 1 of this task

If you want to set the "ONNS Paths Auto Retrieval" (p. 6-47) installation parameter back to **NO**, follow the instructions in Step 1 , by specifying **NO** in step 3.

To run this tool manually, use the "Run the Discover ONNS Paths Tool Manually" (p. 34-9) task.

Task

Complete the following steps to run the Discover ONNS Paths Tool automatically.

1 When prompted using the "Modify an Installation Parameter" (p. 6-167) task, select the following options:

1. Select **Connection Variables**.
2. Select **ONNS Paths Auto Retrieval**.
3. Select **Yes**.
4. Select **y** to accept the change.
5. Select **q** to quit.

2 From the machine on which the management system is running, log in as `oms`.

3 Enter the following command line to invoke the tool:

```
discoverONNSpaths.oms
```

Result: The tool creates two types of log files upon completion. See “Discover ONNS Paths tool logs” (p. 34-4) for details.

END OF STEPS

Run the TDM services move Tool

When to use

Use this task to run the TDM services move Tool.

Related information

See the following topics in this document:

- “ TDM services move tool definition and functionality” (p. 34-5)
- “TDM services move tool pre-conditions” (p. 34-5)
- “TDM services move tool functional requirements” (p. 34-6)

Before you begin

- Run the Network Connections database synchronization on all the NEs to pick up all the connections from the network that may have been set up from the CIT.
- Run the discover ONNS paths script to discover the route details of any Stale connections.

Task

Complete the following task to run the TDM services move tool.

1 Enter the following command line to invoke the TDM services move command-line tool :

```
mv_tdm NE_TID PortAID
```

Where:

`NE_TID` is the TID of the LambdaUnite on which the port resides.

`PortAID` is the Customer/Client PortID from which the traffic needs to be moved.

Result: The TDM services move tool is invoked. If the user enters an NE name that is not of NE Type LambdaUnite or portID (PTP) that is not a Customer/Client port, the script will display an error message.

2 The tool creates the create file(s) and delete file(s) for the connections found.

The format of the files are as follows:

```
<LU TID>_<portAID>_<timestamp>_create.txt
```

```
<LU TID>_<portAID>_<timestamp>_delete.txt
```

Where:

`<LU TID>` is the TID of the source NE of the connection.

`<portAID>` is the Customer/Client PortID.

`<timestamp>` is the date and time the file was generated in the format of DDMMYYHHMMSS.

Note: DD is the day of the month, MM is a two-digit representation of the month, YY is the last two digits of the year, HH is the hour in 24-hour format, MM is the minutes and SS is the seconds.

If the connections are of ASTN Protection Type of Network or Permanent 1+1 Protected with ASTN Protection Mode = RVR, two separate files with protection group commands to make the connections RVR shall be created (one for the source NE and one for the sink NE) in addition to the create/delete files in the following format

`<LU TID>_<portAID>_<timestamp>_createPG.txt`

For example:

- **LUNITE-A_1-1-#-#-32-1_260807212506_create.txt** is created for a user input customer/client port 1-1-#-#-32-1 with all the commands that is needed to create the connections, but without the TID.
- **LUNITE-A_1-1-#-#-32-1_260807212506_delete.txt** is created for a user input customer/client port 1-1-#-#-32-1 with all the commands that is needed to delete the existing connections, but will not contain the TID.
- **LUNITE-A_1-1-#-#-32-1_260807212506_createPG.txt** is created for a user input customer/client port 1-1-#-#-32-1 with the protection group command and another file is created for the other end of the connection(s) with the protection group command.

3 Upon successful completion of Step 2. (create and delete file(s) are successfully created), you can modify the create file(s).

Result: The tool creates a new file, with the user modifications, in the same directory with the same file extensions (create or createPG).

4 Using the OMS GUI ->Tools->TL1 Macro Files, you can execute the delete file(s) or the create file(s) and perform the following:

- In the Search panel, the user can choose the NE Type as LambdaUnite TSS. The resulting files are displayed in the TL1 Macro Files window. The user can View/Modify, Delete or Broadcast.
- If the user chooses to Modify, a new file of the same type will be created. If the user chooses to Broadcast, the user is given the option to enter the NE type (LambdaUnite TSS), the NE name and the filename.

- To delete the existing connections, the user can choose the delete file and the TID to which the delete commands need to be sent. Once the deletes are successful, the user should manually clean up the resulting Improper Disconnect connections from the OMS GUI.
- To create new connections, the user can choose the create file and the TID to which the create commands need to be sent.
- The TL1 broadcast response will display the progress of the commands.
- If any of the commands fail, the user can go to the NWC list and select the appropriate action to make the command successful, or the user can re-try the command from the macro builder.

Note:

- The OMS does not flag errors other than what is displayed in the response area of the macro builder.
- The OMS does not flag errors if the user sends the create commands before the delete commands.

END OF STEPS

35 Non-managed NEs

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the command line tools that assist with non-managed network elements (NEs).

Contents

Non-managed NE Concepts

Non-managed NEs

A non-managed NE is used to represent a network element or a sub-network that is not under the control of OMS, but needs to be represented on the management system in order to have an end-to-end view of circuits in the managed network.

Example: If OMS managed two rings of NEs that were interconnected via an unmanaged SDH network, a non-managed NE could be used to represent the unmanaged network in order to provide an end-to-end view of a connection that starts in one ring and terminates in the other.

Command line tools for non-managed NEs

The management systems offers the following two command-line tools for non-managed NEs:

- "The Bulk Addition of Non-managed NEs" (p. 35-3), which is executed as **ea_import_bb_nes**
- "Modify Cross-Connections in an Non-managed NE" (p. 35-4), which is executed as **OmsLoadXc**. Through its menu items or through its command line parameter specifications, the **OmsLoadXc** tool enables the bulk addition or bulk deletion of specified cross-connections.

Both of these command line tools work in conjunction with a user-specified input file that names the non-managed NEs to be added or the cross-connections in the non-managed NEs that are to be added or deleted.

Non-managed NEs tool supported platforms

The Non-managed NEs tools, which consists of **ea_import_bb_nes** and **OmsLoadXc**, are supported on the *Server Platforms*. The Non-managed NEs tools are also supported on the *PC Platform*.

Non-managed NEs tool licensing

Both tools (**ea_import_bb_nes** and **OmsLoadXc**) are part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute either tool.

The Bulk Addition of Non-managed NEs

ea_import_bb_nes functional overview

The bulk addition of non-managed NEs to OMS is facilitated through the use of a command-line tool called **ea_import_bb_nes**. Users must provide a file containing a list of non-managed NEs to be added to the management system. The tool adds as many of the non-managed NEs that are listed in the file as possible.

ea_import_bb_nes input file

The Bulk Addition of Non-managed NEs command line tool (**ea_import_bb_nes**) works in conjunction with a user-supplied, text file that contains the name of the non-managed NEs to be added. The following conditions apply:

- Each non-managed NE to be added should appear on a separate line in the file and should be a valid non-managed NE name.
- The name of each non-managed NE to be added must be a valid non-managed NE name.

ea_import_bb_nes verifications

Once started, the Bulk Addition of Non-managed NEs command line tool verifies the following conditions:

- The correct user (oms) must be executing the tool.
- The management system platform must be up and running.
- The file containing the list of non-managed NEs must be readable.

Once the tool is running, it verifies the following for each non-managed NE to be added:

- The name of the non-managed NE is a valid name.
- A node with the name of the non-managed NE does not already exist.

If either of these conditions are not met, the tool outputs an error message and continues on to the next listed non-managed NE name.

ea_import_bb_nes log file

The Bulk Addition of Non-managed NEs command line tool (**ea_import_bb_nes**) creates the following log file while the running:

/var/opt/lucent/logs/upgrade/<filename>

Where: **filename** is the name that the tool assigns to the log file. The tool notifies the user of the filename when the tool commences execution.

ea_import_bb_nes related tasks

Refer to the “Run the Bulk Addition of Non-managed NEs Command-Line Tool” (p. 35-13) task for details.

Modify Cross-Connections in an Non-managed NE

OmsLoadXc functional overview

In general, OMS manages the cross connections present in non-managed NEs automatically when connections are created and deleted. However, if a network connection auto-discovery must be performed on a network that has non-managed NEs, the cross connections in the non-managed NEs must be added manually so the management system can discover an end-to-end path. To aid in this manual task, OMS provides the **OmsLoadXc** tool.

The **OmsLoadXc** command line tool can be executed through either of the following methods:

- Via *menu options* in which the tool prompts the user to select a particular menu option. See “OmsLoadXc menu options” (p. 35-4) for details.
- Via *command-line mode* in which the user enters the **OmsLoadXc** command followed by a list of parameter options. See “OmsLoadXc command-line parameter options” (p. 35-4) for details.

OmsLoadXc menu options

The following menu options are available when the **OmsLoadXc** command line tool is executed without specifying any parameter options:

1 - Load cross connects from a file into OMS.

2 - Delete cross connects given in the file from OMS.

3 - Forcefully delete cross connects given in the input file from OMS.

4 - Delete ALL cross connects of an NE given in the input file from OMS.

5 - Forcefully delete all the cross connects of an NE given in the input file from OMS.

99 - exit

OmsLoadXc command-line parameter options

The following command-line parameter options are available when the **OmsLoadXc** command line tool is executed with parameter options:

```
OmsLoadXc -h -d -D -n -x -f <full path of the input file>
```

Where:

-h, which means to request help with the command-line parameter options.

-f <full path of the input file>, is non-interactive mode, which means to run the command in command-line mode using the full-path of the specified file

-d, which means to delete cross-connections

-D, which means to force delete cross-connections

-n, which is to delete cross connections using the NE name data input that is listed in the file

-x, which is to delete the cross-connections using the TP data input that is listed in the file.

Typical usage of the command as it equates to the menu options is as follows:

Command-line Options	Equivalent Menu Options
-f <filename>	Option 1
-d -n -f <filename>	Option 2
-D -n -f <filename>	Option 3
-d -x -f <filename>	Option 4
-D -x -f <filename>	Option 5

OmsLoadXc command-line tool input file

OmsLoadXc uses a text input file to tell it which cross connections are to be added or deleted.

The format and contents of the input file depend on the mode being used:

- When adding or deleting individual cross-connections, the input file is a list of cross connections that are formatted as described in "OmsLoadXC Input File Specifications" (p. 35-7).
- When deleting all cross-connections from a non-managed NE, the input file is a list of non-managed NEs, with one NE listed per line.

OmsLoadXc command-line tool log file

The Management of Cross-Connections in Non-managed NEs command line tool creates the following log file while the running:

/var/opt/lucent/logs/oms/tools/loadxc/<filename>

Where: **filename** is the name that the tool assigns to the log file. The tool notifies the user of the filename when the tool commences execution.

OmsLoadXc Bulk Additions of Cross-Connections

Methods of Specification for OmsLoadXc Bulk Addition of Cross-Connections

The bulk addition of cross-connections to an existing non-managed NE is accomplished via specification of one of the following methods:

- **OmsLoadXc** select > **Option 1**
- **OmsLoadXc -f <filename>**

Verifications for OmsLoadXc Bulk Addition of Cross-Connections

While the tool is loading data from the input file, it verifies the following for each cross connection that is to be added:

- The line in the supplied file is formatted correctly.
- The non-managed NE that is specified exists.
- The Termination Points (TPs) that are specified are available for cross connection.

If any of these conditions are not met, the tool outputs an error message and continues on to the next listed cross connection.

While the tool is loading data from the input file, it automatically creates any TPs that are required to create the cross-connection.

OmsLoadXc Bulk Deletions of Cross-Connections

Methods of specification for OmsLoadXc Bulk Deletion of a Set of Cross-Connections

Once the user provides a file that lists the cross connections to be deleted, the **OmsLoadXc** tool enables the deletion of a set of cross-connections to an existing non-managed NE. The deletion is made specified through of one of the following methods:

- To delete all cross-connections (XCs) in the file from the OMS database that are not used in a connection, one of the following would be specified:
  OmsLoadXc select > **Option 2**
  OmsLoad Xc -d -n -f <filename>
- To delete all cross-connections in the file from the OMS database, whether or not they are used in a connection, one of the following would be specified:
  OmsLoadXc select > **Option 3**
  OmsLoad Xc -D -n -f <filename>

- To delete all cross-connections for a specific NE from the OMS database that are not in use in a connection, one of the following would be specified:
  OmsLoadXc select > **Option 4**
  OmsLoadXc -d -x -f <filename>
- To delete all cross-connections in the file from the OMS database, whether or not they are used in a connection, one of the following would be specified:
  OmsLoadXc select > **Option 5**
  OmsLoadXc -D -x -f <filename>

Verifications for OmsLoadXc Bulk Deletion of a Set of Cross-Connections

The following tool options delete cross-connections from the management system database:

- For all modes in which the system removes individual cross connections, the management system verifies the following:
  —The existence of the cross-connection in the OMS database.
  —When the force option is NOT used, the cross connection is not currently used in a connection.
- For all modes in which the system removed all cross-connections on a non-managed NE, the system verifies the existence of the NE in the OMS database.

OmsLoadXC Input File Specifications

OmsLoadXc Cross-Connections input file

The user must provide a file that contains a list of cross connections to be added or deleted. The tool attempts to add or delete as many of the listed cross connections as possible.

The input file is a text file that contains multiple lines, with one cross-connection per line.

For Cross-Connection Type Data, each line consists of the following data:

```
NE_NAME

XC_RATE

XC_DIRECTION

SHAPE
```

For TP data and for each involved TP, each line consists of the following data:

```
PTP_RATE
```

```
PTP_NAME

FTP_NAME

CTP_NAME

TP_DIRECTION
```

Each line is constructed by presenting the data in the following order. Each field is separated by a **|** (which is a **pipe**) character.

`<Cross Connection Type> <A1 TP Data> <Z1 TP Data> <A2 TP Data> <Z2 TP Data>`

A comment can be added to the file by starting a new line with the **#** (which is the **pound**) character. The comment remains in effect until the end of the line.

`# This is a sample how to add a comment to one line of the input file.`

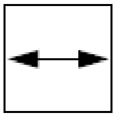
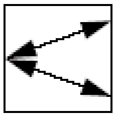
`# This is a sample how to add a comment to the next line in the input file.`

Applicable Values	
PTP Rate	DSR_140M DSR_45M DSR_34M DSR_2M DSR_1_5M STM256 STM64 STM16 STM4 STM1 STM0

Applicable Values	
XC_RATE	VC4_256c VC4_64c VC4_16c VC4_4c AU4_VC4 AU3, TU3_VC3 TU2_VC2 TU12_VC12 TU11_VC11
DIRECTION	BID, UNI*
SHAPE	SIMPLE (A1,Z1) ADD_DROP_A (A1,Z1,A2) INTERCONNECT (A1,Z1,A2)* DOUBLE_ADD_DROP (A1,Z1,A2,Z2) * Refer to“OmsLoadXc Cross-Connections input file SNC shapes” (p. 35-9) for a diagram.
TP Name Fields	Refer to“OmsLoadXc Cross-Connections input file TP naming rules” (p. 35-10) for details.
TP_DIRECTION	BID, UNI*
* Not supported in this release.	

OmsLoadXc Cross-Connections input file SNC shapes

The following diagram illustrates the supported SNC shapes:

sncType	SNC Shape
Simple	
ADD_DROP_A	

OmsLoadXc Cross-Connections input file TP naming rules

PTP name fields must adhere to the rules specified on the **Add Port** page of the management system.

FTP/FTP names are not supported in this release.

PTP Rates adhere to the following for SDH:

SDH PTPs	Rate
STM-0	STM0
STM-1	STM1
STM-16	STM16
SMT-64	STM64
STM256	STM256

PTP Rates adhere to the following for PDH:

PDH PTPs	Rate
1.5 Mbit/s	DSR_1_5M
2 Mbit/s	DSR_2M
34 Mbit/s	DSR_34M
45 Mbit/s	DSR_45M
140 Mbit/s	DSR_140M

CTP naming rules adhere to the following for CTPs that are derived from SDH ports:

CTPs Derived from SDH Ports		
Type	CTP Name	Comment

AU3	/sts1_au3-j=X-k=Y	X = AU4 number
		Y = AU3 number inside AU4

AU4	/sts3c_au4-j=X	X = AU4 number
AU4-4c	/sts12c_vc4_4c=X	X = AU4-4c number
AU4-16c	/sts12c_vc4_16c=X	X = AU4-16c number
AU4-64c	/sts12c_vc4_64c=X	X = AU4-64c number

TU12	/sts3c_au4-j=W/vt2_tu12-k=X-l=Y-m=Z	W = AU4 number
		XYZ = klm number

CTPs Derived from SDH Ports		
Type	**CTP Name**	**Comment**

TU3	/sts3c_au4-j=W/vt2_tu12-k=X-l=0-m=0	W = AU4 number
		X00 = klm number

CTP naming rules adhere to the following for CTPs that are derived from PDH ports:

CTPs Derived from PDH Ports	
VC-11 from 1.5 Mbit/s	/vt15_tull=1
VC-12 from 2 Mbit/s	/vt2_tu12=1
VC-3 from 45 Mbit/s	/tu3_vc3=1
VC-4 from 140 Mbit/s	/sts3c_au4=1

OmsLoadXc Sample cross-connection data input file

```
#-------------------------------------------------------
#
# This is an example of Cross Connect Data File #
#
NE_NAME|XC_RATE|XC_DIRECTION|SHAPE|A1_PTP_RATE
 |A1_PTP_NAME|A1_FTP_NAME|A1_CTP_NAME|A1_TP_DIRECTION
 |Z1_PTP_RATE|Z1_PTP_NAME|Z1_FTP_NAME|Z1_CTP_NAME
 |Z1_TP_DIRECTION|A2_PTP_NAME|A2_PTP_RATE|A2_FTP_NAME
 |A2_CTP_NAME|A2_TP_DIRECTION|Z2_PTP_RATE|Z2_PTP_NAME
 |Z2_FTP_NAME|Z2_CTP_NAME|Z2_TP_DIRECTION
#
#
# Create an Add/Drop connection on BTH-BBOX between:
#  the first VC-4 on Port LP2
#  the first VC-4 from Port A-1 (drop side)

#  the first VC-4 from Port LP1.1

BTH-BBOX|AU4_VC4|BID|ADD_DROP_A|STM1|LP2.1|

 |/sts3c_au4-j=1|BID|A-1||/sts3c_au4-j=1|BID

 |STM1|LP1.1||/sts3c_au4-j=1|BID||||
```

Run the Bulk Addition of Non-managed NEs Command-Line Tool

When to use

Use this task to run the Bulk Addition of Non-managed NEs command-line tool.

Related information

See the following topics in this document:

- "Non-managed NE Concepts" (p. 35-2)
- "The Bulk Addition of Non-managed NEs" (p. 35-3)

Before you begin

Create a text file that contains a list of the non-managed NEs that are to be added to the management system. Refer to "ea_import_bb_nes input file" (p. 35-3) for details.

The execution of the tool requires the management system to be up and running; no loss of network management occurs during execution of the tool.

Task

Complete the following steps to run the Bulk Addition of Non-managed NEs command-line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command line to invoke the Bulk Addition of Non-managed NEs command-line tool:

```
ea_import_bb_nes <neFile>
```

Where: <neFile> is the name of the file that you created that contains a list of the non-managed NEs that are to be added to the management system. Refer to "ea_import_bb_nes input file" (p. 35-3) for details.

> **Result:** The tool performs its verifications and outputs the name of the log file that it has created.

END OF STEPS

Run OmsLoadXc

When to use

Use this task to run the OmsLoadXc command-line tool to modify the cross-connections in non-managed NEs.

Related information

See the following topics in this document:

- "Non-managed NE Concepts" (p. 35-2)
- "The Bulk Addition of Non-managed NEs" (p. 35-3)
- "OmsLoadXc Bulk Additions of Cross-Connections" (p. 35-6)
- "OmsLoadXc Bulk Deletions of Cross-Connections" (p. 35-6)
- "OmsLoadXC Input File Specifications" (p. 35-7)

Before you begin

Create a text file that contains a list of the modifications that are to be made. Refer to "OmsLoadXC Input File Specifications" (p. 35-7) for details.

The execution of the tool requires the management system to be up and running; no loss of network management occurs during execution of the tool.

Task

Complete the following steps run the **OmsLoadXc** command-line tool to modify the cross-connections in non-managed NEs.

1 From the machine on which the management system is running, log in as **`oms`**.

2 To work in the menu driven mode of the tool, refer to "OmsLoadXc menu options" (p. 35-4) for directions and enter the following command line to invoke the **OmsLoadXc** tool:

```
OmsLoadXc
```

To work in the command-line mode of the tool, refer to "OmsLoadXc command-line parameter options" (p. 35-4) for directions and enter the following command line to invoke the **OmsLoadXc** tool:

```
OmsLoadXc
```

OmsLoadXc -h -d -D -n -x -f <full path of the input file>

Result: If you are working in the menu driven mode of the tool, the tool prompts you to supply a menu option.

Depending on whether you are performing a bulk addition of cross connections or a bulk deletion of cross connections, the tool performs the validations that are explained in the following sections: "Verifications for OmsLoadXc Bulk Addition of Cross-Connections" (p. 35-6) and "Verifications for OmsLoadXc Bulk Deletion of a Set of Cross-Connections" (p. 35-7).

END OF STEPS

36 Bulk Renaming of Connections

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the Bulk Renaming of Connections command line tool.

Contents

Bulk Renaming of Connections Concepts

Bulk Renaming of Connections functional overview

The Bulk Renaming of Connections command line tool, which is executed as **OmsModifyConnParams**, enables the OMS user to rename the connection names that were generated through path discovery to the actual connection names that network operations personnel use. This ability to rename connections in bulk is a time saver because each discovered connection no longer has to be renamed, one-by-one, via the management system GUI. Users must provide a simple text file that lists the particular connections to be renamed.

OMS supports the capability to rename connection names in accordance with the following:

- Connection names can be renamed directly from the GUI due to operational needs.
- Connection names can be renamed if they are discovered by OMS through neighbor discovery (for digital links and OTSs).
- Connection names can be renamed by executing the path discovery tool.

In certain situations, such as when OMS is installed on an existing network or when OMS is replacing a classic management system, all existing network connections might have to be inventoried by executing the path discovery tool. Since the path discovery tool generates its own connection name for every discovered path, the **OmsModifyConnParams** tool can be used to change all the path discovery tool generated connection names to the actual connection names that the network operations personnel must use.

Bulk Renaming of Connections tool supported platforms

The Bulk Renaming of Connections tool is supported on the *Server Platforms*. The Bulk Renaming of Connections tool is also supported on the *PC Platform*.

Bulk Renaming of Connections tool licensing

The Bulk Renaming of Connections tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Bulk Renaming of Connections tool functional requirements

The Bulk Renaming of Connections tool adheres to the following functional requirements:

- The tool can be invoked from the command line of HP® server on which the management system is running. The tool is executed while the management system is up and running.
- Only the OMS user who has **oms** user permissions can execute the tool.
- The tool cannot change the connection name format.
  For example, if the existing connection name is in free format, the new name cannot be changed to Telcordia or M1400 format.
- Only one execution of the tool is allowed at a time. Multiple concurrent executions of the tool are not allowed.
- Renaming the connection name does not rename the Connection Alias.
- After the execution of the tool, all management system pages (screens) must be refreshed/re-queried to reflect the new connection names.
- The tool can be used to rename connection names for a SONET or SDH network.
- The input file to the tool can contain records (parameter specifications) for any supported connection rate and can be mixed in any order.

Bulk Renaming of Connections modes of operations

The Bulk Renaming of Connections for OMS is facilitated through the use of a command-line tool called **OmsModifyConnParams**. Users must provide a file containing a list of particular connections to be renamed. Using this file, the tool attempts to perform the requested operation on as many connections that are listed in the file as possible.

The **OmsModifyConnParams** command line tool can be executed through either of the following methods:

- Via *command-line mode* in which the user enters the **OmsModifyConnParams** command followed by a list of parameter options. See "Bulk Renaming of Connections command-line parameter options" (p. 36-3) for details.
- Via *menu options* in which the tool prompts the user to select a particular menu option. See "Bulk Renaming of Connections menu options" (p. 36-4) for details.

Bulk Renaming of Connections command-line parameter options

The following command-line parameter options are available when the **OmsModifyConnParams** command line tool is executed with parameter options:

OmsModifyConnParams -h -m -n -o -f < input file name with full directory path>

Where:

-h is specified to display command usage.

-f, which is optional, is used when the user specifies the input file in the command line. The input file name must be specified with the complete path to the file using the UNIX path naming convention.

-m, which is optional, is used to validate the existence of a connection with both A and Z nodes and ports of every record in the input file. Without this option, the tool only validates the existence of a connection with one edge node and edge port.

-n, which is optional, is used to rename the circuits that were originally in Navis NMS and were migrated to OMS using auto path discovery tool. If specified, the tool processes the additional fields in the input file, which include customer name, priority, comments from Navis® NMS, layout number from Navis® NMS, and the current access code (CAC) from Navis® NMS.

-o, which is optional, is used only to generate the mapping files required to map Navis® NMS layout # and Navis® NMS CAC fields for Navis® PM-MRP and the Dynamic Network Analyzer (DNA), respectively.

If specified, the tool generates the following two output files:

- **snc-name-mapping** is used to map the layout number from Navis® NMS to the connectionID in OMS. This file contains the layout# data (from the input file) and the connectionID data (from OMS database) separated by a **|** (pipe) character. Each line in the file corresponds to one connection record from the input file. The file is located in the following directory:
  /opt/lucent/upgrade/bin
- **cac-to-stackid** is used to map CAC from Navis® NMS to stackID in OMS (for use by DNA). This file contains the CAC (circuit access code) from the input file and the stackID (from the OMS database) separated by **|** (pipe) character. Each line in the file corresponds to one connection record from the input file. The file is located in the following directory:
  /opt/lucent/upgrade/bin

Bulk Renaming of Connections menu options

The following menu options are available when the **OmsModifyConnParams** command line tool is executed without specifying the **-f** parameter option:

```
1) Modify Connection Names using input from a file

99) Exit
```

With specification of option 1, the tool closes the screen and prompts the user to enter the complete path name of the input file.

With specification of option 99, the tool terminates further execution and closes the screen.

Bulk Renaming of Connections tool validations

The Bulk Renaming of Connections tool performs the following validations:

- The command line must be correctly entered with case sensitive characters.
- Only one instance of the tool can be executed at one time.
- If the -f optional parameter is specified, the input file must be accompanied by its exact path.
- If the -n parameter is specified, the tool updates the OMS database with the customer name, priority, and comments from Navis® NMS for the appropriate connection from the input file data.
- The OMS system must be up and running.

If any of the above validations fail, the tool outputs an appropriate error message. If the validations are successful, the tool proceeds with its execution.

Bulk Renaming of Connections log file

The Bulk Renaming of Connections command line tool (**OmsModifyConnParams**) creates the following log files:

- An activity log file
  The activity log file contains the following lines:
  - The starting date and time.
    Example:
    ```
    Bulk Renaming of connections tool execution started on
    2006, August 2, 15:30:21
    ```
  - The result of the execution.
    Example:
    ```
    210 connections are successfully renamed.
    ```
  - The tool completion date and time.
    Example:
    ```
    Bulk Renaming of connections tool execution completed on
    2006, August 2, 15:35:13
    ```
- An error log, which contains the name of the connection that failed to be updated. (The failure could be a validation error or a system failure that occurred during the update.)
- A processed log file, which contains the name of the connection that the tool successfully processed.

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/Bulk_rename

The names of the log files include the date and the time of their creation. For example:

Bulk_rename_activityLog.yyyy.mm.dd.hh.mm.ss

Bulk_rename_errorLog.yyyy.mm.dd.hh.mm.ss

Bulk_rename_processLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

Bulk Renaming of Connections Input File

Bulk Renaming of Connections input file overview

The input file for the Bulk Renaming of Connections tool must adhere to the following specifications:

- It must be a plain text ASCII text file.
- It can consist of multiple lines.
- The input file can contain commented lines starting with a "#" character in the first column for the user notes/instructions.
- Each non-commented line should reflect one record for a connection rename without any carriage return/line feed.

Bulk Renaming of Connections input file parameters

The position of parameters (records) in input file for the Bulk Renaming of Connections tool must adhere to the following specifications:

- Each parameters in the input file is position dependent; therefore, if a parameter is not required it must be skipped after populating a **null** character (no white space).
- Every parameter in the record must be separated by a "|" (pipe) character.

Each non-commented record in the input file should be of the following format:

```
Status(reserved for tool use)|New Connection Name|New Connection
Name format(future)|connection
rate|aNode|aNativeName|comments|zNode|zNativeName|comments|Customer name|pr
```

Where:

1. **Status** is reserved for tool use only and cannot be populated with any character in the input file. The tool copies the record in the Error Log after populating an error message code in this field, which enables the tool to be re-executed using the error log file as an input file after any errors in the input data have been corrected.
2. **New Connection Name** is the new connection name for the required connection. It must be in the same format as the existing connection. The characters in the connection name are case sensitive and must comply with the allowed characters for OMS including any special Latin characters.
3. **New Connection Name format** is reserved for future use to enable the renaming among different connection formats (free, Telcordia, M1400). Any value entered in this field is currently ignored.
4. **Connection rate** is the connection rate of the existing connection name. The rate of an existing connection cannot be changed.
5. **aNode** is the NE name at the A location of the connection. For open ended (Y-protected) connections, this field must represent the termination of the service segment.

6. **aNativeName** is the network element (NE) port address of the connection at the A location of the connection. For open ended (Y-protected) connections, this field must represent the termination of the service segment.
7. **comments** is an optional user field for the A location and port. Validations or processing do not occur.
8. **zNode** is the network element name (NE) at the Z location of the connection. For open ended (Y-protected) connections, this field must represent the termination of the service segment.
9. **zNativeName** is the network element (NE) port address of the connection at the Z location of the connection. For open ended (Y-protected) connections, this field must represent the termination of the service segment.
10. **comments** is an optional user field for the Z location and port. Validations or processing do not occur.
11. **customer name** is an optional parameter used to designate the customer name for the renamed circuit. This field is generally used only when renaming circuits that were originally provisioned in Navis® NMS and are later migrated to OMS through the Connection Auto Discovery Tool.
12. **priority** is an optional field that is used to designate some user specified priority for a connection that was originally provisioned in Navis® NMS and later migrated to OMS through the Connection Auto Discovery Tool.
13. **comments from NMS** is an optional field that contains all of the comments related to the particular circuit from Navis® NMS records.
14. **layout number from NMS** is used to generate a mapping file for Navis® PM-MRP to convert the sncNames in Navis® NMS to the OMS generated sncNames.
15. **cac from NMS** is used for generating a mapping file for DNA to map the CAC field in Navis® NMS to stackID field in OMS.

Bulk Renaming of Connections input file validations

The Bulk Renaming of Connections tool performs the following validations on each record in the input file that is not a comment (does not start with **#** character).

- The connection name must be unique and must not already be used for the specified connection rate by any existing connection in OMS.
- The connection rate must be a valid and supported OMS rate.
- The edge node(s) must exist in OMS, which are both the A and Z nodes when the **-m** parameter is specified in the command line.
- The edge port address(es), which are both the A and Z ends when the **-m** parameter is specified in the command line, must exist for that node.
- A connection with the specified edge nodes, edge ports, and connection rate must exist in OMS.

- The matched connection in **aNode** is in either the **In-Effect** or **Pending** state. It cannot be in the **History** state.
- The first reserved field and the **comments** fields are ignored during processing.

If the tool discovers any errors during the validation process, it logs the error and continues to proceed with the next record.

If the validations are successful, the tool updates the existing connection name with the new connection name and proceed to the next record until every record is examined.

Bulk Renaming of Connections sample input file

```
#--------------------------------------------------------

# Connection Renaming for <customer name> network

myNewConnName||VC-4|LU-A|1-1-#-#-4-16||LU-Z

|1-1-#-#-35-1-25||citibank|7|private line to HQ

|1234567|abcdefg

...

...

|myNewName||VC-4|ADMU-A|TP1.1,2||ADMC-Z|TP4.1,1

|mercedez|9|Munich data center|1236789|abcpqrs
```

Run the Bulk Renaming of Connections Command-Line Tool

When to use

Use this task to run the Bulk Renaming of Connections command-line tool.

Related information

See the following topic in this document:

- "Bulk Renaming of Connections Concepts" (p. 36-1)
- "Bulk Renaming of Connections Input File" (p. 36-6)

Before you begin

Create a text file that contains a list of the connections that are to be renamed. Refer to "Bulk Renaming of Connections Input File" (p. 36-6) for details.

The Bulk Renaming of Connections command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the Bulk Renaming of Connections command line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /var/opt/lucent/logs/oms/tools/Bulk_rename
```

3 To work in the menu driven mode of the tool, refer to "Bulk Renaming of Connections menu options" (p. 36-4) for directions and enter the following command line to invoke the **OmsModifyConnParams** tool:

```
OmsModifyConnParams
```

To work in the command-line mode of the tool, refer to "Bulk Renaming of Connections command-line parameter options" (p. 36-3) for directions and enter the following command line to invoke the **OmsModifyConnParams** tool:

```
OmsModifyConnParams -h -m  -f < input file name with full
directory path>
```

Result: If you are working in the menu driven mode of the tool, the tool prompts you to supply a menu option.

The tool performs the validations that are explained in "Bulk Renaming of Connections tool validations" (p. 36-4) and "Bulk Renaming of Connections input file validations" (p. 36-7).

END OF STEPS

37 Ethernet

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the command line tools that are associated with Ethernet management.

Contents

Bulk Renaming of Ethernet Services Concepts

Bulk Renaming of Ethernet Services functional overview

The Bulk Renaming of Ethernet Services command line tool, which is executed as **OmsModifyEthernetParams**, enables the OMS user to rename Ethernet Services to accommodate operational needs or to rename a service that OMS discovered through executing the Ethernet resynchronization process.

In certain situations, such as when OMS is installed on an existing network or when OMS replaces a classic management system, all existing Ethernet services might have to be inventoried by executing the Ethernet resynchronization process. Since the Ethernet resynchronization process generates its own names for every new service, users can execute the **OmsModifyEthernetParams** tool to change all of the Ethernet resynchronization process-generated service names to the service names that they actually use. By using the **OmsModifyEthernetParams** tool to rename the Ethernet services in bulk, instead of renaming each discovered service using the GUI for one service at a time, users can save valuable time.

Bulk Renaming of Ethernet Services tool supported platforms

The Bulk Renaming of Ethernet Services tool is supported on the *Server Platforms*. The Bulk Renaming of Ethernet Services tool is not supported on the *PC Platform*.

Bulk Renaming of Ethernet Services tool licensing

The Bulk Renaming of Ethernet Services tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Bulk Renaming of Ethernet Services tool functional requirements

The Bulk Renaming of Ethernet Services tool adheres to the following functional requirements:

- The tool can be invoked from the command line of HP® server on which the management system is running. The tool is executed while the management system is up and running.
- Only the OMS user who has **oms** user permissions can execute the tool.
- Only one execution/instance of the tool is allowed at a time. Multiple concurrent executions of the tool are not allowed.
- After the execution of the tool, all management system pages (screens) must be refreshed/re-queried to reflect the new service names.
- The input file to the tool can contain records (parameter specifications) for any supported Ethernet service.

Bulk Renaming of Ethernet Services modes of operations

The Bulk Renaming of Ethernet Services for OMS is facilitated through the use of a command-line tool called **OmsModifyEthernetParams**. Users must provide a file containing a list of particular Ethernet Services to be renamed. Using this file, the tool attempts to perform the requested operation on as many Ethernet Services that are listed in the file as possible.

The **OmsModifyEthernetParams** command line tool can be executed through either of the following methods:

- Via *command-line mode* in which the user enters the **OmsModifyEthernetParams** command followed by a list of parameter options. See "Bulk Renaming of Ethernet Services command-line parameter options" (p. 37-3) for details.
- Via *menu options* in which the tool prompts the user to select a particular menu option. See "Bulk Renaming of Ethernet Services menu options" (p. 37-3) for details.

Bulk Renaming of Ethernet Services command-line parameter options

The following command-line parameter options are available when the **OmsModifyEthernetParams** command line tool is executed with parameter options:

OmsModifyEthernetParams -h -f < input file name with full directory path>

Where:

-h is specified to display command usage.

-f, which is optional, is used when the user specifies the input file in the command line. The input file name must be specified with the complete path to the file using the UNIX path naming convention.

Bulk Renaming of Ethernet Services menu options

The following menu options are available when the **OmsModifyEthernetParams** command line tool is executed without specifying the **-f** parameter option:

```
Modify Ethernet Parameters Menu

1) Modify Ethernet Service names using input from a file

99) Exit

Enter selection:
```

With specification of option 1, the tool prompts the user to enter the complete path name of the input file.

With specification of option 99, the tool terminates further execution and closes the screen.

Bulk Renaming of Ethernet Services tool validations

The Bulk Renaming of Ethernet Services tool performs the following validations:

- The command line must be correctly entered with case sensitive characters.
- Only one instance of the tool can be executed at one time.
- If the `-f` optional parameter is specified, the input file must be accompanied by its exact path.
- The OMS system must be up and running.

If any of the above validations fail, the tool outputs an appropriate error message. If the validations are successful, the tool proceeds with its execution.

Bulk Renaming of Ethernet Services log file

The Bulk Renaming of Ethernet Services command line tool (**OmsModifyEthernetParams**) creates the following log files:

- An activity log file

  The activity log file contains the following lines:

  – The starting date and time.

    Example:

    ```
    Bulk Renaming of Ethernet Services tool execution started on
    2006, August 2, 15:30:21
    ```

  – The result of the execution.

    Example:

    ```
    <x> Ethernet Services were successfully renamed.
    ```

    Where: x is the number of Ethernet Services that were successfully renamed.

  – The tool completion date and time.

    Example:

    ```
    Bulk Renaming of Ethernet Services tool execution completed
    on
    2006, August 2, 15:35:13
    ```

- An error log, which contains the name of the service that failed to be updated.
  Example:

  ```
  Service not found|EPL 1|N||AMU001|LAN1.1|MegaBank|For a
  private line
  ```

- A processed log file, which contains the `New Service Name` of the each service that the tool successfully renamed.

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/Bulk_Ethernet_rename

The names of the log files include the date and the time of their creation. For example:

Bulk_Ethernet_rename_activityLog.yyyy.mm.dd.hh.mm.ss

Bulk_Ethernet_rename_errorLog.yyyy.mm.dd.hh.mm.ss

Bulk_Etherent_rename_processLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files. The log files are not automatically purged.

Bulk Renaming of Ethernet Services Input File

Bulk Renaming of Ethernet Services input file overview

The input file for the Bulk Renaming of Ethernet Services tool must adhere to the following specifications:

- It must be a plain text ASCII text file.
- It can consist of multiple lines.
- It can contain commented lines starting with a "#" character in the first column for the user notes/instructions. The line must be terminated with a carriage return.
- Each non-commented line must reflect one record, which is a string of parameter specifications that contain the current information for the renaming of the Ethernet service. The line must be terminated with a carriage return.
- A carriage return must be used to terminate one complete line; a carriage return cannot be used in the middle of any line that contains a record or a comment.

Bulk Renaming of Ethernet Services input file parameters

The position of parameters, which are also known as *records*, in the input file for the Bulk Renaming of Ethernet Services tool must adhere to the following specifications:

- Each parameters in the input file is position dependent; therefore, if a parameter is not required it must be skipped after populating a **null** character (no white space).
- Every parameter in the record must be separated by a "|" (pipe) character.
- To skip a parameter, nothing must appear between two "|" (pipe) characters. Example:
  ```
  ||
  ```

Each non-commented record in the input file must adhere to the position-dependent format for following parameters:

```
Status (reserved for tool use)|New Service Name|Service
Type|VLAN ID|LAN Port Network Element|LAN Port Name|Customer
Name|Comments
```

Where:

1. **Status** is reserved for tool use only and cannot be populated with any character in the input file. The tool copies the record in the error log after populating an error message code in this field, which enables the tool to be re-executed using the error log file as an input file after any errors in the input data have been corrected.
2. **New Service Name** is the new service name for the Ethernet service.

3. **Service Type** is a single character that represents the type of Ethernet service as follows:
   `N` represents non-switched Ethernet service.
   `V` represents a virtual switch network.
   `S` represents a switched Ethernet service.
   `H` represents a hub-and-spoke Ethernet service.
4. **VLAN ID** is the VLAN ID for the service, which is only required if the user specifies a switched service (service type = **`S`**).
5. **LAN Port Network Element** is the NE name of any LAN port in the Ethernet service.
6. **LAN Port Name** is the port name of any LAN port in the Ethernet service. It is the same LAN port that is specified for the LAN Port Network Element parameter.
7. **Customer Name** is an optional user parameter that is used to specify the name of the customer.
8. **Comments** is an optional user parameter that the user can use to specify any notes regarding a particular record or the input file in general.

Bulk Renaming of Ethernet Services input file validations

The Bulk Renaming of Ethernet Services tool performs the following validations on each record in the input file that is not a comment (does not start with **#** character).

- The LAN Port Network Element, the LAN Port Name, and the Customer Name must valid names in OMS.
- If the Service Type is switched service (**`S`**), the VLAN ID must be a number from 1 to 4093.
- The Service Type must be a valid Ethernet service type, which is the following:
  `N` for a non-switched Ethernet service.
  `V` for a virtual switch network.
  `S` for a switched Ethernet service.
  `H` for a hub-and-spoke Ethernet service.
- The New Service Name must be a valid Ethernet service name and it cannot already be used as the service name for any other Ethernet service.

If the tool discovers any errors during the validation process, it logs the error and continues to proceed with the next record.

If the validations are successful, the tool updates the existing service name with the new service name and proceeds to the next record until every record is examined.

Bulk Renaming of Ethernet Services sample input file

The following is a sample of an input file that can be used for the Bulk Renaming of Ethernet Services tool:

```
|EPL 1|N||AMU001|LAN1.1|MegaBank|For a private line

|VSN 1|V||AMU001|LAN2.1||For a VSN

|VLAN 1|S|1|AMU001|LAN2.1|MiniBank|For VLAN ID 1

|VLAN 2|S|2|AMU001|LAN2.1|MiniBank|For VLAN ID 2, on the same port

#This is an example of an entire line that is a comment.

#

#Comments can also be included as the last parameter

#(field) in a record (line).

#For example:  "For a private line"

#is a comment in the first record.
```

Tools for moving Ethernet services from one card to another card

Ethernet services move tools definition and functionality

OMS provides a pair of command-line tools that you can use to “move” the Ethernet services from one card to another. The tools are:

- **Export Ethernet Service Tool:** Creates a file, which describes the Ethernet service
- **Create Ethernet Service Tool:** Inputs a file and creates a service in the system as described by the contents of the file

Notes

- The tools are limited to only Non-switched Private Line services
- The tools are part of the **OMS_CORE** license. A separate license is not needed to execute the tool

When combined with “Tool for moving TDM services from one card (NE) to different card (NE) ” (p. 34-5), the overall workflow is as follows:

1. Execute the `mv_tdm` script to build the command template for moving the VCG.
2. Execute the `mv_eth_export` script to save the description of the Ethernet service.
3. Edit the files created above, as needed.
4. DB Delete the Ethernet service using the OMS GUI.
5. Execute the commands for deleting the VCG.

6. DB Delete the VCG connection and/or inconsistent connections as a result of the above action, as needed.
7. Execute the commands for creating the VCG.
8. Execute the `mv_eth_create` script to build the new Ethernet service.

Ethernet services move tools functional requirements

The following functional requirements apply to the successful execution of the Ethernet Service Move tool:

- The tools can be invoked from the command line of the HP® server on which the management system is running. The tools are executed while the management system is up and running.
- Only the OMS user who has OMS user permission can execute the tool.
- Only one execution of each of the tools are allowed at a time. Multiple concurrent executions of the tools are not allowed.

Run the Bulk Renaming of Ethernet Services Command-Line Tool

When to use

Use this task to run the Bulk Renaming of Ethernet Services command-line tool.

Related information

See the following topic in this document:

- "Bulk Renaming of Ethernet Services Concepts" (p. 37-1)
- "Bulk Renaming of Ethernet Services Input File" (p. 37-5)

Before you begin

Create a text file that contains a list of the Ethernet Services that are to be renamed. Refer to "Bulk Renaming of Ethernet Services Input File" (p. 37-5) for details.

The Bulk Renaming of Ethernet Services command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the Bulk Renaming of Ethernet Services command line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 To work in the menu driven mode of the tool, refer to "Bulk Renaming of Ethernet Services menu options" (p. 37-3) for directions and enter the following command line to invoke the **OmsModifyEthernetParams** tool:

```
OmsModifyEthernetParams
```

To work in the command-line mode of the tool, refer to "Bulk Renaming of Ethernet Services command-line parameter options" (p. 37-3) for directions and enter the following command line to invoke the **OmsModifyEthernetParams** tool:

```
OmsModifyEthernetParams -f <input file name with full directory
path>
```

Result: If you are working in the menu driven mode of the tool, the tool prompts you to select a menu option.

In either mode of operation, the tool performs the validations that are explained in "Bulk Renaming of Ethernet Services tool validations" (p. 37-3) and "Bulk Renaming of Ethernet Services input file validations" (p. 37-6).

If the tool detects any errors, go to Step 3.

3 If the tool detects any errors, examine the error file.

If needed, update the actual error file to resolve the errors.

Go to Step 2 and re-run the tool using the corrected error file as input.

END OF STEPS

Run the Export Ethernet Service Tool

When to use

Use this task to run the export Ethernet Service Tool.

Related information

See the following topic in this document:

- "Ethernet services move tools definition and functionality" (p. 37-7)
- "Ethernet services move tools functional requirements" (p. 37-8)

Before you begin

This task does not have any pre-conditions.

Task

Complete the following task to run the export Ethernet service tool.

1 Enter the following command line to invoke the Export Ethernet Service command-line tool :

`mv_eth_export <NE_name> <port_AID>`

Where: **`<NE_name>`** is the name of the Network Element and **`<port_AID>`** is the access identifier for the VCG port at that end of the VCG.

For example:

mv_eth_export LUNITEC 1-1-#-#-12-v1

Result: The system validates the content of the input file.

If there are no errors, the system generates an ASCII text file containing the description of the service.

The format of the file is as follows:

```
SERVICE_CLASSIFICATION=Non-switched
SERVICE_TYPE=Private Line
A_END_NE=name of the NE at the A end of the service
A_END_PORT=LAN port name at the A end of the service
Z_END_NE=name of the NE at the Z end of the service
Z_END_PORT=LAN port name at the Z end of the service
ETHERNET_CAPABLE_LINK=name of the VCG in the service
```

```
CUSTOMER_NAME=customer name of the service

SERVICE_NAME=name of the service
```

The output file name is as follows:
`<NE_name>_<port_AID>_<timestamp>_export_eth.txt`

Where:

`<NE_name>` is the name of the input Network Element.

`<port_AID>` is the name of the input port AID.

`<timestamp>` is the date and time the file was generated in the format of YYMMDDHHMMSS.

Note: YY is the last two digits of the year, MM is a two-digit representation of the month, DD is the day of the month, HH is the hour in 24-hour format, MM is the minutes and SS is the seconds.

For example:

The file **LUNITEC_1-1-#-#-12-v1_070608143427_export_exh.txt** will contain:

```
SERVICE_CLASSIFICATION=Non-switched

SERVICE_TYPE=Private Line

A_END_NE=LUNITEC

A_END_PORT=1-1-#-#-12-1

Z_END_NE=LUNITED

Z_END_PORT=1-1-#-#-14-3

ETHERNET_CAPABLE_LINK=My_VCG

CUSTOMER_NAME=My_Customer

SERVICE_NAME=EPL0034
```

If there are errors in the input, an error message is displayed and the script exits; no ASCII text file will be created.

END OF STEPS

Run the Create Ethernet Service Tool

When to use

Use this task to run the Create Ethernet Service Tool.

Related information

See the following topic in this document:

- "Ethernet services move tools definition and functionality" (p. 37-7)
- "Ethernet services move tools functional requirements" (p. 37-8)

Before you begin

An ASCII text file describing the Ethernet service must be created on the OMS host.

Task

Complete the following task to run the Create Ethernet service tool.

1 Enter the following command line to invoke the Create Ethernet Service command-line tool :

```
mv_eth_create <filename>
```

Where: **<filename>** is the full path to a text file containing the description of an Ethernet service.

For example:

```
mv_eth_create /tmp/LUNITEC_1-1-#-#-12-v1_070608143427_export_exh.txt
```

Result: The system validates the content of the input file and creates an Ethernet service matching the description in the input file.

If there are errors in the input, an error message is displayed and the script exits.

END OF STEPS

38 Bulk Upload of Digital Link and Connections

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the Bulk Upload of Digital Link and Connections command line tool.

Contents

Bulk Upload of Digital Links and Connections Concepts

The need for a tool for digital links and connections

In general, topological links, which are also referred to as digital links, are the physical transport connection between two adjacent network elements (NEs). The physical port at both ends of the link determines the rate of the topological link. Generally, in OMS, these topological links can either be discovered using one of two methods:

- By using the capabilities of the NEs that can discover their neighbors.
- By using a tool to upload the digital links into OMS database and/or the physical connections that already exist in the network.

In addition, the use of a tool would enable a user to bulk provision topological/digital links so that user would not have to enter the data in a one-by-one manner through the management system GUI.

Bulk Upload of Digital Link and Connections functional overview

The Bulk Upload of Digital Link and Connections command line tool, which is executed as **OmsBulkUpld**, enables the OMS user to perform a bulk upload of a digital link and connections to the Navis® Optical Management System or to bulk provision a digital link and connections to the Navis® Optical Management System.

This tool can be executed using one of two modes:

- The **bulk upload** mode supports the upload of digital links for all rates that OMS supports. Use of the bulk upload mode is similar to creating digital links during database synchronization through neighbor discovery because the port provisioning commands are not sent to the NEs.
- The **bulk provisioning** mode supports digital links for all rates that OMS supports and, for 1675 Lambda Unite MultiService Switch (MSS), the bulk provisioning of TDM connections for all rates that OMS supports. Use of the bulk provisioning mode is similar to having users provisioning the digital links from the management system GUI as **add** orders. The port provisioning commands for this mode of execution are sent to the NEs.

When executed, the tool simulates the provisioning of topological links as if they were added individually through the management system GUI. In addition, the error detection during the tool execution is as complete as the validation that the management system GUI and host perform.

Bulk Upload of Digital Link and Connections tool supported platforms

The Bulk Upload of Digital Link and Connections tool is supported on the *Server Platforms*. The Bulk Upload of Digital Link and Connections tool is also supported on the *PC Platform*.

Bulk Upload of Digital Link and Connections tool licensing

The Bulk Upload of Digital Link and Connections tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Bulk Upload of Digital Link and Connections tool functional requirements

The Bulk Upload of Digital Link and Connections tool adheres to the following functional requirements:

- The tool can be invoked from the command line of HP® server on which the management system is running. The tool is executed while the management system is up and running.
- Only the OMS user who has **oms** user permissions can execute the tool.
- Only one execution of the tool is allowed at a time. Multiple concurrent executions of the tool are not allowed.

- The tool cannot be executed in bulk upload and bulk provisioning modes at the same time.
- All the NEs in the network including Black Boxes are inventoried in management system before executing the tool.
- The synchronization for ports and protection groups on all the NEs are successfully performed before the execution of the tool.
- When executing the tool in bulk provisioning mode, the management system is communicating with all NEs. Appropriate port or cross-connect provisioning commands might have to be sent if the cross-connects are not derived from the uncorrelated cross-connect records.
- When executing the tool in bulk upload mode, all ports belonging to the digital links must have already been put into service (or laser on the OTs turned on for OS links) or verified to be “in service” to enable reporting of alarms. The ports must be substructured appropriately to carry higher order SDH connections, such as AU3 or VC4. Port or cross-connect commands are not sent to the NEs.
- The tool supports the following types of topological links for SDH/SONET digital links and topological links at the optical layer:
  - unprotected
  - 1+1 MSP protected
  - 1x1 MSP protected for all network elements and all connections at the optical layer (OMS, OCH, and OCN-RS/STM-nRS)
- The tool does not support the bulk upload or bulk provisioning of performance monitoring on the topological links that are supported. Users must set and collect performance monitoring data through the management system GUI after the digital links are inventoried in the management system.

Bulk Upload of Digital Link and Connections modes of operations

The Bulk Upload of Digital Link and Connections for OMS is facilitated through the use of a command-line tool called **OmsBulkUpld**. Users must provide a file containing a list of particular connections to be renamed. Using this file, the tool attempts to perform the requested operation on as many connections that are listed in the file as possible.

The **OmsBulkUpld** command line tool can be executed through the *command-line mode* in which the user enters the **OmsBulkUpld** command followed by a list of parameter options. See “Bulk Upload of Digital Link and Connections command-line parameter options” (p. 38-3) for details.

Bulk Upload of Digital Link and Connections command-line parameter options

The following command-line parameter options are available when the **OmsBulkUpld** command line tool is executed with parameter options:

OmsBulkUpld -t<dl/connections>, -m<add/upload>, -v, -f < input file name with full directory path>

Where:

-t < > is the connection type, which can be **dl** (digital link) or **connections**

-m < > is the provisioning mode, which can be **add** or **upload** for bulk upload. (For cross-connect based connection provisioning, only the **add** mode is supported.)

-v, which is applicable for digital links only, is to validate the input records in accordance with the validation criteria. Any errors in validation are logged in a log file.

Note: When **-v** is specified, the user wants to validate the data in the input file and is currently restricted to digital links. The tool performs the following validations without sending the requests to the Order Handler for further processing. All required fields in the input line must be present. For example, fields, such as prot_conn_name, prot_association_name are not required for 1+1 MSP digital links. The optional fields, which are those fields in which the system populates the values, are not checked. The conn_rate is a valid connection rate. The NE TIDs and the ports are valid TIDs and ports in the management system database. The connection name, if provided in the input file, is unique. The digital link cannot already exist in management system database for the specified input data (NE and ports).

-f < > is the full path name to the input file.

Bulk Upload of Digital Link and Connections tool order types

Based on the arguments and the options in the command line, the following order types are created for all records from the input file:

- In the non-interactive mode, the arguments -t, -m, and -f are mandatory along with appropriate specified parameter values.
- For argument **-m** with option **upload**, the order type created in the management system is **Discovered**.
- For argument **-m** with option **add**, the order type created in the management system is **Add**.

Bulk Upload of Digital Link and Connections tool validations

The Bulk Upload of Digital Link and Connections tool performs the following validations:

- The command line must be correctly entered with case sensitive characters.
- Only one instance of the tool can be executed at one time.
- If the -f optional argument is specified, the input file must be accompanied by its exact path.
- The OMS system must be up and running.

If any of the above validations fail, the tool outputs an appropriate error message. If the validations are successful, the tool proceeds with its execution.

Bulk Upload of Digital Link and Connections log file

The Bulk Upload of Digital Link and Connections command line tool (**OmsBulkUpld**) creates the following log files:

- An activity log file
  The activity log file contains the following lines:
  - The starting date and time.
    Example:
    ```
    Bulk Upload of Digital Link and Connections tool execution
    started on
    2006, August 2, 15:30:21
    ```
  - The number of records in the input file.
  - The number of records executed/implemented successfully.
  - The number of records that failed the implementation or failed by the system to create the connection record successfully.
  - The number of records that failed in the validation before giving it to the system.
  - The tool completion date and time.
    Example:
    ```
    Bulk Upload of Digital Link and Connections tool execution
    completed on
    2006, August 2, 15:35:13
    ```
- The Error Log contains records from the input file that failed during validation or implementation. Each line in the error log copies the input record and updates the **status** (first field) field with the error message. The error message displays the first error in which the system encountered and stopped further processing of that record.
- A processed log file contains the details of the successfully completed connections along with the record number, connection name (working), connection name (protection) as provided in the input data, followed by a blank line and followed by Order Status, Order Number, Connection Name (working), Order step (InEffect) for all successfully completed connections. For 1x1 MSP digital links, the order status, order number and connection name (protection) are also provided.

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/bulkupld

The names of the log files include the date and the time of their creation. For example:

activityLog.yyyy.mm.dd.hh.mm.ss

errorLog.yyyy.mm.dd.hh.mm.ss

processedConnectionLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

Bulk Upload of Digital Link and Connections re-execution of the tool

The Bulk Upload of Digital Link and Connections tool enables users to re-execute the tool in one of two methods:

- By re-using (or copying) the error log as the input file after updating the input data based on the error messages that were generated.
- By creating a new input file and re-running the tool.

For the system failed errors that are logged in the Error Log, users can remove the data record from the input file and use the management system GUI to re-send or force complete the implementation. If the error log contains several records for which global substitution is required, users can fix those errors in the input file and re-run the tool.

Bulk Upload of Digital Link and Connections Input File

Bulk Upload of Digital Link and Connections input file overview

The input file for the Bulk Upload of Digital Link and Connections tool must adhere to the following specifications:

- Each input file must be a plain text ASCII text file that has a unique filename.
- Each input file can consist of multiple lines.
- Each input file can contain commented lines starting with a “#” character in the first column for the user notes/instructions. Any commented line is not processed
- Any record that contains a blank line without any white spaces except a carriage return (**Return** or **Enter**) is not processed.
- Each non-commented line should reflect one record for a connection rename without any carriage return/line feed.
- Each digital link/connection record shall be completely contained in one line.
- Each line can wrap-around as appropriately needed. Hyphens cannot be used to break the words when wrapping around.
- Each field in the record is position dependent, which means, if a field is not applicable, the field should be a null character (not a white/blank space).
- Each field in the record is separated by a **|** or **tab** character and both **|** or **tab** character cannot be used anywhere else in the record. Within one record, the delimiters **|** or **tab** cannot be mixed.

Bulk Upload of Digital Link and Connections input file parameters

The position of parameters (records) in input file for the Bulk Upload of Digital Link and Connections tool must adhere to the following specifications:

- Each parameters in the input file is position dependent; therefore, if a parameter is not required it must be skipped after populating a **null** character (no white space).
- Every parameter in the record must be separated by a **|** (pipe) character or a **tab** key.

Each non-commented record in the input file should be of the following format:

1. **status** is reserved for tool use only and cannot be populated with any character in the input file. The tool uses this parameter to populate the error followed by the input data of the failed record.
2. **record_no** is the record number in the input file.
3. **connection_name** is the connection name or circuit ID. The system generates a connection name, if one is not found in the input data.
4. **connection_alias** is the same as connection name if it is not populated. The system generates a connection alias, if not given in the input data.
   Important! If the system level parameter for **connection alias** is OFF, the system still generates and populates the **connection alias** and **protection connection alias** fields in the database. Since the system parameter is OFF, the user cannot see these fields in the management system GUI displays.
5. **fromNE1** is the TID of the NE/Black Box at the A1 location.
6. **fromNE2** is the TID of the NE/Black Box at the A2 location for a three-ended adddrop A connection. It is not applicable for digital links.
7. **toNE1** is the TID of the NE/Black Box at the Z1 location.
8. **toNE2** is the TID of the NE/Black Box at the Z2 location for a three ended adddrop Z connection. It is not applicable for digital links.
9. **fromport1** is the port address, which is the working port address for a 1+1 or 1x1 MSP at fromNE1 end.
10. **fromport2** is the port address, which is the protection port address for a 1+1 or 1x1 MSP at fromNE1 end.
11. **toport1** is the port address, which is the working port address for MSP) at toNE1 end.
12. **toport2** is the port address, which is the protection port address for a 1+1 or 1x1 MSP at toNE1 end.
13. **conn_rate** is the connection rate.
    For digital links, connection rates can be any of the following:
    OC1, OC3, OC12, OC48, OC192, OC768 or STM1, STM4, STM16, STM64, STM256
    For connections, SDH rates, which conform to the rates internal to the OMS application, are any of the following:
    AU4_VC4, VC4_4c, VC4_16c, TU3_VC3, TU12_VC12

14. **protection_type** is the protection type.
    For digital links it is unprotected and 1+1MSP.
    For connections, it is unprotected
    The default is **unprotected** for both digital links and connections when not populated in the input file.
15. **substructuring**, which is applicable for VC4/STS1 connections (up to three characters), is **Yes**, **No**, or null (empty field with no white space).
16. **prot_conn_name** is the protection connection ID for 1+1 MSP digital links. The system generates a protection connection name if one is not supplied in the input data.
17. **prot_conn_alias** is the alias for protection connection name for both 1+1 MSP and 1x1MSP digital links. The system generates a connection alias if one is not supplied in the input data.
18. **prot_association_name** is the Protection Association Name for both 1+1 MSP and 1x1 MSP digital links. The system generates a protection association name if one is not supplied in the input data.
19. **order_number**, which is optional, is the number that is associated with the order. The system creates one if this field is null.
20. **customer_name**, which is optional, is the name of the customer. The system creates one if this field is null.
21. **comments**, which is optional, is the comments field. This field cannot contain the delimiter character (**|** or **tab**). The system leaves this field blank if it is not populated.
22. **routing_mode** is cross-connect.
23. **overall connectionshape** can be SIMPLE (bi), ADD_DROP_A (bi), ADD_DROP_Z (bi), DOUBLE_ADD_DROP (bi).
24. **category** is ManagedPlane, which is the default.
25. **ServiceType** is DS3, Undetermined, or NA (default).
26. **ne1 tid** is the TID of NE1.
27. **ne1 cross-connect shape** can be SIMPLE, ADD_DROP_A, ADD_DROP_Z, or DOUBLE_ADD_DROP.
28. **ne1fromport1** is the from port of the working port at NE1. It can be up to 50 characters.
29. **ne1fromport2** is the from port of protection at NE1 for 1+1 path protection that has ADD_DROP_A at NE1. It can be up to 50 characters.
30. **ne1toport1** is the to port of the working port at NE1.
31. **ne1toport2** is the to port of protection at NE1 for 1+1 path protection that has ADD_DROP_Z at NE. It can be up to 50 characters.
32. **ne2tid** is the TID of NE2 for logical connections only. It can be up to 20 characters.
33. **ne2 cross-connect shape** can be SIMPLE, ADD_DROP_A, ADD_DROP_Z, or DOUBLE_ADD_DROP.

34. **ne2fromport1** is the from port of the working port at NE2. It can be up to 50 characters.
35. **ne2fromport2** is the from port of protection at NE2 for 1+1 path protection that has ADD_DROP_A at NE2. It can be up to 50 characters.
36. **ne2toport1** is the to port of the working port at NE2.
37. **ne2toport2** is the to port of protection at NE2 for 1+1 path protection that has ADD_DROP_Z at NE2 It can be up to 50 characters.

Bulk Upload of Digital Link and Connections input file validations

The Bulk Upload of Digital Link and Connections tool performs the following validations on each record in the input file that is not a comment (does not start with **#** character).

- The text file must exist in OMS in the specified location either in the command line argument **-f** or when prompted in interactive mode.
- Each field of data in each line must be separated by **|** (pipe) or **tab** character.
- Since the data is read from the input file, default values are generated only for the fields specified in the input file contents.
- Each line (each record) must contain all required fields.
- For each record from the input file, an input XML structure and IDL is created and sent to the appropriate subsystem (OH).

If the tool discovers any errors during the validation process, an appropriate error message is logged in the error log file, further execution of the tool for that record is terminated, and the system proceeds with the processing of the next input data.

During the execution of the tool, each input line is processed. If a failure to implement or a failure to upload the data in OMS occurs because of validation failures or implementation failures (such as a time out or a communication failure with the NE), the tool logs the error in the Error Log and continues processing the next record in the input file. The tool terminates when all the input lines are processed.

Run the Bulk Upload of Digital Link and Connections Command-Line Tool

When to use

Use this task to run the Bulk Upload of Digital Link and Connections command-line tool.

Related information

See the following topic in this document:

- "Bulk Upload of Digital Links and Connections Concepts" (p. 38-1)
- "Bulk Upload of Digital Link and Connections Input File" (p. 38-6)

Before you begin

Create a text file that contains a list of the digital links or connections that are to be uploaded or provisioned using this tool. Refer to "Bulk Upload of Digital Link and Connections Input File" (p. 38-6) for details.

The Bulk Upload of Digital Link and Connections command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the Bulk Upload of Digital Link and Connections command line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /opt/lucent/logs/oms/tools/bulkupld
```

Result: You are now in the **bulkupld** directory.

3 Enter the following command line to invoke the **OmsBulkUpld** tool and refer to "Bulk Renaming of Connections command-line parameter options" (p. 36-3) for directions:

```
OmsBulkUpld -t<dl/connections>, -m<add/upload>, -v,  -f < input
file name with full directory path>
```

Result: The tool performs the validations that are explained in "Bulk Upload of Digital Link and Connections tool validations" (p. 38-4) and "Bulk Upload of Digital Link and Connections input file validations" (p. 38-9).

END OF STEPS

39 Bulk Database Delete

Overview

Purpose

This chapter contains the conceptual information and the related tasks that are needed to run the Bulk Database Delete command line tool.

Contents

Bulk Database Delete Concepts

Bulk Database Delete functional overview

The Bulk Database Delete command line tool, which is executed as **bulk_DBdelete**, enables the OMS user to perform a database deletion of a number of connections/multiplex sections.

The following scenarios exhibit the instances in which the database deletion of multiple connections going through or terminating on a network element can be used:

- Moving an NE that is outside a ring (either PSR or MSSPRING) into the ring by refibering the existing ring.
- Reconfiguring an NE from STM-16 to STM-64 on the high speed ports and inserting that NE into a STM-64 fiber ring.
- Regrouping VC12s in a MSSRPING ring and consolidating them into fewer VC4s, thereby freeing the other VC4s.

- Swapping an NE with another NE planned fiber cut by temporarily adding protection to unprotected circuits and removing protection after the maintenance activity is completed.
- Temporarily adding protection to unprotected circuits and removing that protection after the maintenance activity is completed on a planned fiber cut.

Bulk Database Delete tool supported platforms

The Bulk Database Delete tool is supported on the *Server Platforms*. The Bulk Database Delete tool is also supported on the *PC Platform*.

Bulk Database Delete tool licensing

The Bulk Database Delete tool is part of the "OMS_CORE license" (p. 5-5). A separate license is not needed to execute the tool.

Bulk Database Delete tool functional requirements

The Bulk Database Delete tool adheres to the following functional requirements:

- The tool can be invoked from the command line of HP® server on which the management system is running. The tool is executed while the management system is up and running.
- Only the OMS user who has **oms** user permissions can execute the tool.
- The tool is applicable to SDH, SONET, and optical layer connections and links.
- Only one execution of the tool is allowed at a time. Multiple concurrent executions of the tool are not allowed.
- All the circuits/digital links that are to be database deleted are **In-Effect**.
- The user must supply an input file that works in conjunction with the tool. The tool rearranges that input file into a usable format.
- All performance monitoring data is lost for the connection names specified in the input file.
- Since the database delete functionality in the management system does not allow the database deletion of a connection ID if the connection ID has any client paths/trails, the tool does not perform any related validations.

Bulk Database Delete mode of operation

The Bulk Database Delete for OMS is facilitated through the use of a command-line tool called **bulk_DBdelete**. Users must provide a file containing a list of the particular connections to database deleted. The tool rearranges that input file into a usable format. Using this rearranged input file, the tool attempts to perform the requested operation on as many connections that are listed in the file as possible.

The **bulk_DBdelete** command line tool can be executed through the *command-line mode* in which the user enters the **bulk_DBdelete** command followed by a parameter. See "Bulk Renaming of Connections command-line parameter options" (p. 36-3) for details.

Bulk Database Delete command-line parameter

The following command-line parameter is available when the **bulk_DBdelete** command line tool is executed:

bulk_DBdelete -f <input file name with full directory path>

Where:

-f is used to specify the full path of the input file using the UNIX path naming convention.

Bulk Database Delete tool validations

The Bulk Database Delete tool performs the following validations:

- The command line must be correctly entered with case sensitive characters. The command line must be specified with the **-f** parameter.
- Only one instance of the tool can be executed at one time.
- When the **-f** parameter is specified, the input file must be accompanied by its exact path.
- The OMS system must be up and running.

If any of the above validations fail, the tool outputs an appropriate error message. If the validations are successful, the tool proceeds with its execution.

Bulk Database Delete log file

The Bulk Database Delete command line tool (**bulk_DBdelete**) creates the following log files:

- An activity log file
  The activity log file contains the following lines:
  - The starting date and time.
    Example:
    ```
    Bulk DB Delete tool execution started on 2006, August 2,
    15:30:21
    ```
  - The tool completion date and time.
    Example:

```
Bulk DB Delete tool execution completed on 2006, August 2,
15:35:13
```

- An error log, which contains the name of the connection, along with the connection rate in parentheses, that failed to be validated or failed to be deleted from the database.
- A processed log file, which contains the name of the connection, along with the connection rate in parentheses, that the tool successfully processed.

These log files reside in the following directory:

/var/opt/lucent/logs/oms/tools/db_delete

The names of the log files include the date and the time of their creation. For example:

DBDelete_activityLog.yyyy.mm.dd.hh.mm.ss

DBdelete_errorLog.yyyy.mm.dd.hh.mm.ss

DBdelete_processLog.yyyy.mm.dd.hh.mm.ss

The date and time correspond to the creation date and time of the log files. Any subsequent execution of the tool creates additional log files that have a new time stamp. To preserve system space, users must delete all old log files.

Bulk Database Delete Input File

Bulk Database Delete input file overview

The input file for the Bulk Database Delete tool must adhere to the following specifications:

- It must be a plain text ASCII text file.
- It can consist of multiple lines.
- The input file can contain commented lines starting with a **#** character in the first column for the user notes/instructions.
- Each non-commented line should reflect one record for a connection rate without any carriage return/line feed.
- It consists of circuit IDs (connection names) and the connection rate (layer rate) separated by either a tab character or a **|** character, one circuit ID on each line.
- Although the number of circuits to be database deleted in the input file in unlimited, for optimal performance, we suggest that you limit the number of circuits to less than 500 connections.

The connection (layer rate) that is specified in the input file must correspond exactly to the management system GUI labels. The valid rates are as follows

- SDH digital links:
  STM-1, STM-4, STM-16, STM-64, STM-256
- SDH connections:
  VC4-4-64c, VC-4-16c, VC-4-4c, VC-4, LO-VC-3, VC-12
- Ethernet connections:
  —Non-switched Ethernet service, Hub-and-Spoke service, Switched Ethernet service, Virtual Switch Network
  —The Non-switched Ethernet service and the Hub-and-Spoke service must be deleted before their corresponding VCG servers are deleted.
  —The Switched Ethernet service must be deleted before deleting its Virtual Switch Network connection.
  —The Virtual Switch Network connection must be deleted before deleting its corresponding VCG server.
- SONET digital links:
  OC-1, OC-3, OC-12, OC-48, OC-192, OC-768, EC-1
- SONET digital links:
  OC-1, OC-3, OC-12, OC-48, OC-192, OC-768, EC-1
- DWDM links:
  OS, OTS, OMS
- DWDM connections:
  OCH, ODU2.5G, ODU10G, OC-3RS, OC-12RS, OC48-RS. OC-192RS, OC-768RS, DSR

Bulk Database Delete input file validations

The Bulk Database Delete tool performs the following validations on each record in the input file that is not a comment (does not start with **#** character).

- Validations on the circuit IDs (connection names) and/or on the connection rate are performed as each record in the input file is processed for a DB deletion.
- The **comments** fields for blank lines are ignored during processing.

If the tool discovers any errors during the validation process, it logs the error and continues to proceed with the next record.

If the validations are successful, the tool updates the existing connection name with the new connection name and proceed to the next record until every record is examined.

Bulk Database Delete sample input file

The separation between the connection name and the connection rate might appear exaggerated. The separator is a tab character

```
#--------------------------------------------------------

# Connection name         Connection rate

1/VC-12/AM1-SRINI-I/AM1-SRINI-I    VC-12

1/STM-4/AMU-NJ-03/METROU-C          STM-4

1/VC-4/AMU-SR-01/AMU-INDIR-0       VC-4

1/STM-1/AMU-SR-02/AMU-INDIR-0      STM-1

1/STM-1/AMU-SR-02/AMU-SR-01        STM-1

1/STM-1/ISM1/AM1-SRINI-I           STM-1

1/STM-1/ISM_T_1/AM_73              STM-1

1/STM-4/LUNITE-A/LUNITE-B          STM-4

1/VC-4-4c/LUNITE-A/LUNITE-C        VC-4-4c

1/VC-4/LUNITE-A/LUNITE-D           VC-4

1/STM-16/LUNITE-B/LUNITE-D          STM-16

1/STM-4/LUNITE-C/LUNITE-D          STM-4

1/STM-64/LIMBURG/WALLAWALLA        STM-64

1/VC-12/LUNITE-A/LUNITE-B          VC12

1/STM-64/LUNITE-A/LUNITE-C          STM-64

1/VC-4/LUNITE-B/LUNITE-C           VC-4

1/STM-64/LUNITE-C/LUNITE-D          STM-64

1/OS/LXTREME-A/LXTREME-B           OS

1/OCH/LXTREME-A/LXTREME-B          OCH

1/OC48RS/LXTREME-A/LXTREME-B       OC-48RS
```

Bulk Database Delete connection rate mapping table

The following table maps the connection rates on the management system GUI label to internal layer rates in the management system.

GUI display of Connection Rate	Internally Mapped Rate
STM-1	oc3_ms_stm1
STM-4	oc12_ms_stm4
STM-16	oc48_ms_stm16
STM-64	oc192_ms_stm64
STM-256	oc768_ms_stm256
OC-1	oc1_ms_stm0
EC-1	LR_Electrical_EC1_sts1_STM
OC-3	oc3_ms_stm1
OC-12	oc12_ms_stm4
OC-48	oc48_ms_stm16
OC-192	oc192_ms_stm64
OC-768	oc768_ms_stm256
VC-12	vt12_tu12_vc12
LO-VC-3	tu_vc3
VC-4	sts3c_au4_vc4
VC-4-4c	sts12c_vc4_vc4_4c
VC-4-16c	sts48c_vc4_vc4_16c
VC-4-64c	sts192c_au4_vc4_64c
VT1.5	vt1.5_tu11_vc11
VT2	vt2_tu12_vc12
STS-1	sts1_au3
STS-3c	sts3c_au4_vc4
STS-12c	sts12c_vc4_4c
STS-48c	sts48c_vc4_16c
STS-192c	sts192c_vc4_64c
OS	OPTICAL_SECTION
OTS	OTS
OMS	optical_multiplex_section

GUI display of Connection Rate	Internally Mapped Rate
OCH	OCH
ODU2.5G	ODU1
ODU10G	ODU2
DSR	DSR
OC-3RS	section_oc3_sts3_rs_stm1
OC-12RS	section_oc12_sts12_rs_stm4
OC-48RS	section_oc48_sts48_rs_stm16
OC-192RS	section_oc192_sts192_rs_stm64
OC-768RS	section_oc768_sts768_rs_stm256
VCG	fragment

The rearranged input file

The tool copies the input file to a new file and rearranges the records in the new file, which is referred to as the *rearranged input file*.

The records in the rearranged input file are rearranged in the following sequence:

1. low order connections and Ethernet connections
   For example: LO-VC-3/VC-12 or VT1.5/STS-1 low-order service connections
2. high order infrastructure connection
   For example: VC-4 high order infrastructure connections
3. high order service connections
   For example: VC-4, VC-4-4c, VC-4-16c, OCH, ODU2.5G, ODU10G high order service connections
4. multiplexer connections, optical links, and VCGs
   For example: STM-16, STM-64 multiplexer connections
   For example: OS and OMS optical links

Since both 1+1 MSP and 1x1 MSP protected links are provisioned or deleted through group orders, the tool processes only one of these links for deletion. The tool verifies if any digital links in the rearranged input file are 1+1 MSP or 1x1 MSP protected. If any such link is found, the tool verifies if the other link (protection or service) also exists in the rearranged input file. If the other link exists in the rearranged input file, the tool skips that other link. If the other link does not exist, the tool deletes the other link for both the 1+1 MSP and the 1x1 MSP protected links. However, for a 1x1 MSP protected digital link, since the other link could be carrying preemptible traffic, this verification is logged in the Error Log.

Validations on the rearranged input file

For each record in the rearranged input file, the tool performs the following validations:

- The connection name exists in OMS database and it is **In-Effect** for the connection rate specified.
- A pending (**Rearrange**, **Delete**, or **DB Delete**) order for the connection does not exist at or beyond the implementation step (except for **DB Delete** orders).
- The connection rate is a valid rate.
- The rearranged input file does not contain any other fields.

If any validation fails, the tool log the error in the Error Log and proceeds to validate the next record.

If the validation on a record succeeds, the tool performs a database deletion of the appropriate record.

Run the Bulk Database Delete Command-Line Tool

When to use

Use this task to run the Bulk Database Delete command-line tool.

Related information

See the following topic in this document:

- "Bulk Database Delete Concepts" (p. 39-1)
- "Bulk Database Delete Input File" (p. 39-4)

Before you begin

Create a text file that contains a list of the connections that are to be renamed. Refer to "Bulk Database Delete Input File" (p. 39-4) for details.

The Bulk Database Delete command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to run the Bulk Database Delete command line tool.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to change directories:

```
cd /var/opt/lucent/logs/oms/tools/db_delete
```

3 Enter the following command line to invoke the **bulk_DBdelete** tool and refer to "Bulk Renaming of Connections command-line parameter options" (p. 36-3) for directions:

```
bulk_DBdelete  -f < input file name with full directory path>
```

Result: The tool performs the validations that are explained in "Bulk Database Delete tool validations" (p. 39-3) and "Bulk Database Delete input file validations" (p. 39-5).

END OF STEPS

40 Port Assignments

Overview

Purpose

This chapter explains the port assignments that are to be made for the management system.

Contents

Management System Port Assignments

Table of management system port assignments

The following table lists the port assignments for management ports. The service protocol for all ports is TCP.

Service/Port Number	Service Name	Comment
80	N/A	Apache*; GUI Platform; http required port to enable the network firewall for communication between the management system and the client during login.
389	N/A	Lightweight Directory Access Protocol (LDAP) database

Service/Port Number	Service Name	Comment
443	N/A	https required port to enable the network firewall for communication between the management system and the client during login.
1099	N/A	RMI; GUI Platform
1521	ORA Listener	The Oracle® Listener Port; Platform
1812	N/A	RADIUS authentication
1813	N/A	RADIUS accounting
2212	N/A	TIM Interface; OMS Platform
3082	N/A	Reserved port for 1665 DMX Access Multiplexer, 1665 Data Multiplexer Explore (DMXplore), and 1665 DMXtend Access Multiplexer use.
3083	N/A	Reserved for 1625 LambdaXtreme® Transport Security Socket Layer (SSL) use
4000	xipcetc	GUI Platform
4001	xipcserv	GUI Platform
8007	N/A	Apache*/Tomcat Interworking; GUI Platform
8009	N/A	Apache*/Tomcat Interworking; GUI Platform
8080	MRP	Ethernet Provisioning Manager (EPM) to Navis MRP communication
8081	N/A	Tomcat; GUI Platform
8101	N/A	jvm1 Debugging Port; OMS Platform
8102	N/A	jvm2 Debugging Port; OMS Platform
8103	N/A	jvm3 Debugging Port; OMS Platform

Service/Port Number	Service Name	Comment
8104	N/A	jvm4 Debugging Port; OMS Platform
8105	N/A	jvm5 Debugging Port; OMS Platform
8106	N/A	jvm6 Debugging Port; OMS Platform
8107	N/A	jvm7 Debugging Port; OMS Platform
8108	N/A	jvm8 Debugging Port; OMS Platform
8109	N/A	jvm9 Debugging Port; OMS Platform
8111	N/A	pmc_jvm1 Debugging Port
8112	N/A	pmc_jvm2 Debugging Port
8113	N/A	pmc_jvm3 Debugging Port
8114	N/A	pmc_jvm4 Debugging Port
8115	N/A	pmc_jvm5 Debugging Port
8116	N/A	pmc_jvm6 Debugging Port
8117	N/A	pmc_jvm7 Debugging Port
8118	N/A	pmc_jvm8 Debugging Port
8119	N/A	pmc_jvm9 Debugging Port
8146	N/A	LDAP Administration Port
9040	oms_subsys_ctrl_main	Management System Subsystem Controller; OMS Platform
9041	fm_subsys_ctrl	FM Subsystem Controller; OMS platform
9050	tna_subsys_ctrl_main	TNA Subsystem Controller; TL1 Platform
9055	tna_subsys_ctrl	TNA Subsystem Controller Child; TL1 Platform
9056	nma_subsys_ctrl	NMS Subsystem Controller Child
9060	cna_subsys_ctrl_main	CNA Subsystem Controller; CMISE Platform

Service/Port Number	Service Name	Comment
9070	cna2000_ipc_a	CNA Interprocess Communication; CMISE Platform
9071	cna2000_ipc_b	CNA Interprocess Communication; CMISE Platform
9072	cna2000_ipc_c	CNA Interprocess Communication; CMISE Platform
9073	cna2000_ipc_d	CNA Interprocess Communication; CMISE Platform
9074	cna2000_ipc_e	CNA Interprocess Communication; CMISE Platform
9075	cna2000_ipc	CNA Interprocess Communication; CMISE Platform
9076	cna2000_ipc_dyn	CNA Interprocess Communication; CMISE Platform
9077	cna_nai1	CNA M16 Adaptor Port; CMISE Platform
9078	cna_nai2	CNA MADM Adaptor Port; CMISE Platform
9079	cna_nai3	CNA CMUX Adaptor Port; CMISE Platform
9080	cna_nai4	CNA AMU port
9081	cna_nai5	CNA BPM M16 port
9082	cna_nai6	CNA BPM MADM port
9083	cna_nai7	CNA BPM CMUX port
9084	cna_nai8	CNA BPM 1655 Access Multiplexer Universal (AMU) port
9085	cna_uicm	SC MADM port
9086	sc_m16_nai	SC M16 port (for CMISE NE EMS)
9087	sc_cmux_nai	SC CMUX port (for CMISE NE EMS)
9088	sc_a155_nai	SC A155 port (for CMISE NE EMS)
9089	sc_pz_nai	SC PZ port (for CMISE NE EMS)
9090	sc_ism_nai	SC ISM port (for CMISE NE EMS)

Service/Port Number	Service Name	Comment
9091	sc_slm_nai	SC SLM port (for CMISE NE EMS)
9092	sc_m80_nai	SC M80 port (for CMISE NE EMS)
9093	sc_wdacs_nai	SC WDACS port (for CMISE NE EMS)
9095	sc_madm_nai	SC MADM port
9096	N/A	SNA
9097	N/A	SNMP traps for SNMP (LER) NEs
9098	N/A	Command Center
9099	tna_cit	TNA to CIT communication
9170	tna_nai0	TNA - CGW Server Port; TL1 Platform
9171	tna_nai1	South Bound, Security Socket Layer (SB SSL) Command/ Response Port
9172	tna_nai2	South Bound, Security Socket Layer (SB SSL) Autonomous Message Port
9173	tna_nai3	South Bound, Security Socket Layer (SB SSL) FTP Port
9174	tna_nai4	TNA Server Port for BPM Router Client
9175	tna_nai5	TNA - Spare Client Port; TL1 Platform
9176	tna_nai6	TNA - PMC port that is used to listen for cron requests
9177	tna_nai7	TNA - Spare Client Port; TL1 Platform
9178	tna_nai9	TNA - Spare Client Port; TL1 Platform
9180	tna_icp_a	TNA Internal Cmd and/or OSI Communications Static Service A; TL1 Platform

Service/Port Number	Service Name	Comment
9181	tna_icp_b	TNA - Internal TL1 and/or OSI Communications Static Service B; TL1 Platform
9182	tna_icp_c	TNA Internal Cmd and/or TCP/IP Communications Static Service C; TL1 Platform
9183	tna_icp_d	TNA Internal TL1 and/or TCP/IP Communications Static Service D; TL1 Platform
9184	tna_icp_e	TNA Internal Spare Communications Static Service E; TL1 Platform
9185	tna_icp_f	TNA Internal Spare Communications Static Service F; TL1 Platform
9186	tna_icp_g	TNA Remote Server Port
9187	tna_chmod	TNA Change Mode; TL1 Platform
9190	tna_PmcRemote_0	TNA PmcRemote Test Tool
9191	tna_PmcRemote_1	TNA PmcRemote Test Tool
9192	tna_PmcRemote_2	TNA PmcRemote Test Tool
9193	tna_PmcRemote_3	TNA PmcRemote Test Tool
9194	tna_PmcRemote_4	TNA PmcRemote Test Tool
9195	tna_PmcRemote_5	TNA PmcRemote Test Tool
9196	tna_PmcRemote_6	TNA PmcRemote Test Tool
9197	tna_PmcRemote_7	TNA PmcRemote Test Tool
9198	tna_PmcRemote_8	TNA PmcRemote Test Tool
9199	tna_PmcRemote_9	TNA PmcRemote Test Tool
9201	N/A	mount_cdrom
9211	N/A	Load Log Records; Navis® OMS Platform
9212	N/A	File Transfer

Service/Port Number	Service Name	Comment
9213	N/A	File Transfer
9214	N/A	PM cron collection
9215	N/A	Default closed port
9400* to 9499	N/A	CNA Subsystem Controller; CMISE Platform *Note that ports 9400 to 9408 are used for UI and necc gateway communication
9591	N/A	oms_ft
9600	N/A	Bulk Performance Management (BPM) Subsystem Controller Root
9601	N/A	BPM Subsystem Controller Child
9602	N/A	BPM Router Server Port
9603	N/A	BPM Reporter Port
9604	N/A	BPM Spare Port; reserved for future use.
9605	N/A	BPM Spare Port; reserved for future use.
9606	N/A	BPM Spare Port; reserved for future use.
9607	N/A	BPM Spare Port; reserved for future use.
9608	N/A	BPM Spare Port; reserved for future use.
9609	N/A	BPM Spare Port; reserved for future use.
9620	snms_nai	Navis® EMS port
9621	oms_snmp_agent	Simple Network Management Protocol (SNMP) agent port. See “SNMP Interface” (p. 17-5) for details.
9622	cgw_ept	CORBA™ Gateway (CGW) Engineering and Planning Tool (EP&T)

Service/Port Number	Service Name	Comment
9623	XOS_Server	NMA to XOS Server
9624	BPM-NMA	
10160	N/A	Northbound TL1 Alarm Interface
11098	RMI_NS	NMA RMI
11099	Jboss_NS	NMA JBoss
15122	JNDI_Port	NMA JNDI
15123	RMI_Port	NMA RMI
14444	JRMP_Port	NMA JRMP
14445	Pooled_Invoker	NMA Pooled Invoker
18093	UIL2_Port	NMA UIL2
32999	N/A	Used by GUI platform daemon
55000 to 55099	N/A	Orbix® Software; Platform
* This product includes software developed by the Apache Software Foundation (http://www.apache.org/).		

Change the Orbix® Port Number

When to use

Use this procedure to change the Orbix® port number. The default Orbix port number is 55075.

Related information

See the following topic in this document:

- “TMF814 Northbound Interface Configuration and Setup” (p. 18-6)

Before you begin

Important! We do not recommend that you change the Orbix port number unless it is absolutely necessary.

Task

Complete the following steps to change Orbix® port number.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to bring the platform and the GUI web server down:

```
platform_cntrl stop
```

3 Enter the following command:

```
su -root
```

4 Enter the following command to change directories:

```
cd /opt/lucent/orbix_asp
```

5 Enter the following command to copy the **driver.dtd** file:

```
cp orbix_asp_dd.xml orbix_asp_dd.xml.ofc
```

6 Enter the following command to copy the **driver.xml** file:

```
cp orbix_asp_dd_ent.xml orbix_asp_dd_ent.xml.ofc
```

7 Enter the following command to access the file with the **vi** editor:

```
vi orbix_asp_dd.xml
```

8 Find the particular line containing the default port number and change the port number.

9 Save the changes made to the file and exit the file:

```
<Shift> ZZ
```

10 Enter the following command to copy the **driver.dtd** file:

```
cp orbix_asp_dd.xml orbix_asp_dd.ent.xml
```

11 Enter the following command and option to update the IONA Orbix configuration:

```
/opt/lucent/platform/bin/ionarepair
```

Select option **a**.

12 Enter the following command to copy the **locatorMap.xml** file:

```
cp /etc/opt/lucent/locatorMap.xml /etc/opt/lucent/
locatorMap.xml.ofc
```

13 Change all occurrences of 55075 in port number to <n>75 (e.g. 55075 -> 3075).

14 Save the changes made to the file and exit the file:

```
<Shift> ZZ
```

15 Enter the following command to return to the management system OMS login:

```
exit
```

16 Enter the following command to bring up the application and the GUI web server:

```
platform_cntrl start
```

Result: The system returns the message `Subsystem are now available` to inform you that you can proceed to the next step.

17 Enter the following command to bring down the application and the GUI web server:

```
platform_cntrl stop
```

18 Enter the following command to bring up the application and the GUI web server:

```
platform_cntrl start
```

END OF STEPS

Change the Management System Feedback Orbix® Port Number Range

When to use

Use this procedure to change the management system feedback Orbix® port number range.

Related information

See the following topic in this document:

- "Change the Orbix® Port Number" (p. 40-9)

Before you begin

This procedure is specifically intended for the TMF814 Northbound Interface client that is connected to the management system server using the port number range of 55000 to 55099. This procedure should only be used to change the default port number range.

Task

Complete the following steps to change the management system feedback Orbix® port number range.

1 From the machine on which the management system is running, log in as **oms**.

2 Enter the following command to bring the application and the GUI web server down:

```
platform_cntrl stop
```

3 Enter the following command to change directories:

```
cd /etc/opt/iona/domains
```

4 Enter the following command to access the file with the **vi** editor:

```
vi orbix_asp.cfg
```

5 Find the particular line containing the following string:

```
"policies:giop:interop_policy:send_locate_request = "false";
```

6 Insert the following line after the `policies:giop...` line:

```
policies:iiop:server_address_mode_policy:port_range = "<m>:<n>";
```

Where: m is the *from* port number and n is the *to* port number.

7 Save the changes made to the file and exit the file:

```
<Shift> ZZ
```

8 Enter the following command to bring up the application and the web server:

```
platform_cntrl start
```

END OF STEPS

41 System Maintenance

Overview

Purpose

This chapter explains the on-going system maintenance that needs to be performed for the management system and its platforms.

Contents

Daily Housekeeping

Run hot system backups

On a daily basis, run a hot system backup. Refer to "Best time of the day for system and NE backups" (p. 10-4) for specific times and refer to the "Execute an Immediate Hot System Backup from the OMS" (p. 10-8) task for details.

Important! To avoid running housekeeping tasks simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

In addition, the data from any hot system backup that has been done on the Server Platform should be written to tape daily; refer to the "Write a System Backup to Tape " (p. 10-12) task for details. **Important!** If a hot system backup is run daily, the data from the previous day is overwritten. Therefore, if the data is not written to tape or to another device and/or system, the previous day's data is lost.

Refer to "System Backups" (p. 10-2) for more information about the operating principles of backups, the types of backups, hot system backups, system recoveries, and related backup alarms.

Check running services

On a daily basis, check running services to determine if all required processes are functioning. Running services, such as daily cron jobs, might get hung after daily backups. (Two common cron jobs are **lt_cronadmin** and, for High Availability configurations, **lt_ha_cronadmin**.) See "Check Running Services" (p. 9-4) for instructions.

Check platform alarms

On a daily basis, check platform alarms and respond to any alarms that might have occurred.

Refer to Chapter 42, "Platform Alarms" in this document for details.

Check system logs

On a daily basis, check the systems logs, which are located at **/var/adm/syslog**, to determine if any errors have occurred.

Check disk space

On a daily basis, check disk space by using the UNIX® **bdf** command.

Periodic Maintenance

Run cold system backups

Depending on the need, run a cold system backup every week or every two weeks. Refer to "Best time of the day for system and NE backups" (p. 10-4) for specific times and refer to the "Execute a Cold System Backup from the HP® Server" (p. 10-9) task for details.

Important! To avoid running housekeeping tasks simultaneously or at times that are not beneficial to the overall health and functioning of the system, always refer to the recommended time and frequency for scheduled activities that is suggested in the "Table of scheduled activities" (p. 41-4).

Refer to "System Backups" (p. 10-2) for more information about the operating principles of backups, the types of backups, cold system backups, system recoveries, and related backup alarms.

Patches and security updates

Depending on the need, keep patch levels current for all Microsoft® software products that are running in conjunction with the management system. See "Keep patch levels current" (p. 3-3) for details.

Set up new users

When the need arises, set up the PC clients for new users and create their accounts.

Refer to all procedures listed in Chapter 3, "Client Set Up" to perform the necessary software set ups and installations for the PC clients of new users.

Refer to the "Copy a User Role Profile" (p. 7-24) or "Add a User-Defined User Role Profile" (p. 7-25) tasks to assign factory or user-defined user role profiles to the new users and "Add a User Account" (p. 8-15) to create accounts for the new users.

Audit user accounts

Once a month, audit user accounts to locate and remove dead user accounts.

Refer to the "View a List of User Accounts" (p. 8-14) and "Delete a User Account" (p. 8-19) tasks for details.

Determine the latest releases

Once a month, contact your Alcatel-Lucent local customer service support team to determine the *latest releases* of your NEs and the latest releases of the management system that support your NEs. The latest release of the management system might include features, tools, and support services that address your ever-changing network management needs.

The NEs that support the features of the management system documented in this revision of the product and this document are listed in "Summary of supported NEs" (p. 1-5).

Check licenses

If your network is growing rapidly, *check licenses* once a month to determine whether additional licenses are needed.

Bring down and reboot

Every two months on the Server Platform, bring all running processes down and reboot the HP® servers. See "Restart the HP® Servers" (p. 9-13) for details.

For HP® Serviceguard configurations, restart only the standby nodes.

Scheduled Activities

Table of scheduled activities

The following table identifies the recommended time and frequency of scheduled activities that occur within the management system and its operating platform. A scheduled activity is triggered to execute because of settings that are specified in a cron job or an installation parameter.

For more information regarding the nature of installation parameters, refer to "Installation Parameter Concepts" (p. 6-2); to view the settings of an installation parameter, refer to "View the Parameter Settings of an Installation Parameter" (p. 6-165); for the steps needed to change an installation parameter, refer to "Modify an Installation Parameter" (p. 6-167).

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
xx:x0 xx:x5 every 5 minutes	**bpm_db_loader_cron** cron	User: **bpm** Bulk Performance Monitoring (BPM) data processing
On single CPU servers: xx:03 xx:33 xx:53 every 20 minutes ---------------- On multiple CPU servers: xx:x3 every 10 minutes	**fm_alarmevent_purge** cron	User: **oms** Purges old records from the network event summary table.

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
On single CPU servers: xx:06 xx:36 every 30 minutes ---------------- On multiple CPU servers: xx:06 xx:21 xx:36 xx:51 every 15 minutes	**pm_scheduled_stop_cron_15m** cron	User: **oms** Checks for scheduled stops in PM 15-minute monitoring and stops if necessary
On multiple CPU servers: xx:04 xx:34 every 30 minutes	**fm_logsize_monitor** cron	User: **oms** Checks the size of the alarm logs, generating warning alarms and purges records if necessary.
On multiple CPU servers: xx:07 xx:37 every 30 minutes	**fm_tcasize_monitor** cron	User: **oms** Checks the size of the Threshold Crossing Alert (TCA) logs; generates warning alarms, and purges records if needed.
On multiple CPU servers: xx:17 xx:47 every 30 minutes	**fm_alarmsize_monitor** cron	User: **oms** Checks the size of the current Alarms List; generates warning alarms, and purges records if needed.
xx:15 xx:45 every 30 minutes	**cleanup** cron	User: **root** Resource Monitor script that is used to remove old files.
xx:55 hourly	**oh_del_history_order** cron	User: **oms** Starts the deletion of history orders.

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
Hourly from the start	Implemented as a Java™ internal timer.	If needed, log purges of the User Activity Log, NE Notification Log, Command and Response Logs.
11:32 17:32 every 6 hours	**fm_log_suppressed** cron	User: **oms** Collects suppressed alarm and Threshold Crossing Alert (TCA) files from NAs and enters them into the alarm history log.
21:00 Mon/Wed/Fri	**db_monitor** cron	User: **oracle** Database Monitor
On single CPU servers: 21:04 daily	**fm_logsize_monitor** cron	User: **oms** Checks the size of the alarm logs, generating warning alarms and purges records if necessary.
On single CPU servers: 21:17 daily	**fm_alarmsize_monitor** cron	User: **oms** Checks the size of the current Alarms List; generates warning alarms, and purges records if needed.
On single CPU servers: 21:37 daily	**fm_tcasize_monitor** cron	User: **oms** Checks the size of the Threshold Crossing Alert (TCA) logs; generates warning alarms, and purges records if needed.
21:00-22:00 daily		The time that is recommended for an NE backup. This time is user-set.
22:00 daily	**bpm_db_admin_cron** cron	User: **bpm** Housekeeping (purging) of the Bulk Performance Monitoring (BPM) database.
22:05 daily	**fm_suppressed_alarms_cron.oms** cron	User: **oms** Detects suppressed alarms and raises a platform alarm if any are found. For information alarm holding, refer to the *OMS Service Assurance Guide*.

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
22:10 daily	**discoverONNSpaths** cron	User: **oms** Retrieves and resynchronizes with ONNS paths for 1675 Lambda Unite MultiService Switch (MSS).
22:30 daily	**fm_alarm_retention** cron	User: **oms** Purges records from the current Alarms List that are older than the set retention period.
22:40 daily	**fm_log_retention** cron	User: **oms** Purges records from the alarm logs that are older than the set retention period.
22:48 daily	**fm_tca_retention** cron	User: **oms** Purges records from the Threshold Crossing Alert (TCA) log that are older than the set retention period.
22:56 daily	**fm_pse_retention** cron	User: **oms** Purges records from the Protection Switch Event (PSE) log that are older than the set retention period.
23:08 daily	**fm_psesize_monitor** cron	User: **oms** Checks the size of the Protection Switch Event log, generates warning alarms, and purges as necessary.
23:17 every 6 hours	**fm_log_suppressed** cron	User: **oms** Collects suppressed alarm and TCA files from NAs and enters them into the alarm history log
23:30 daily	**DataExtraction** cron	User: **oms** Prepares Data Extraction; creates data files that are ready for collection. See the "Enable/Disable DET Report Cron" (p. 6-120) installation parameter and Chapter 16, "Data Extraction" for details.

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
23:38 daily	**fm_flapping_alarms** cron	User: **oms** Analyses alarm data to detect whether an particular alarm has been raised and cleared many times.
00:05 daily	**lm_client** cron	User: **oms** Start of user activity log, NE notification log, and command and response log collection from the NAs.
00:09 daily	**deleteLocalETHorders** cron	User: **oms** Removes failed Ethernet requests (and related data) that are older than 24 hours.
00:10 daily	**ea_delete_history_nes** cron	User: **oms** Internal housekeeping: removes deleted NEs that had been retained to allow internal synchronization.
00:20 daily	**oh_del_fiber_recovery** cron	User: **oms** Purges the restore complete orders associated with the fibre cut recovery feature.
00:30 daily	**inventory_purge** cron	User: **oms** Purges the XML inventory data.
01:00 daily	**nwc_delete_orphan_xc** cron	User: **oms** Deletes orphaned cross-connects. See the "Orphan Cross Connection Deletion Tool" (p. 6-46) installation parameter for details.
02:00 daily	**prf_purge** cron	User: **oms** The deletion of temporary data that is related to profiles.
02:35 daily	**bpm_pmc_collect_24h** cron	User: **bpm** Bulk Performance Monitoring (BPM) 24 hour data collection.

Time and Frequency	cron Job* or Installation Parameter Trigger	Activity/Comments
03:00 daily	**db_del_inst_alarms** cron	User: **cna** Deletes instaneous alarms in CNA that are older than 24 hours.
On single CPU servers: 03:04 daily	**fm_logsize_monitor** cron	User: **oms** Checks the size of the alarm logs, generating warning alarms and purges records if necessary.
On single CPU servers: 03:17 daily	**fm_alarmsize_monitor** cron	User: **oms** Checks the size of the current Alarms List; generates warning alarms, and purges records if needed.
03:30 daily	**pm_purge** cron	User: **oms** PM age and size purges.
On single CPU servers: 03:37 daily	**fm_tcasize_monitor** cron	User: **oms** Checks the size of the Threshold Crossing Alert (TCA) logs; generates warning alarms, and purges records if needed.
04:00 - 05:00 daily		The time that is recommended for OMS system backup. This time is user-set.
05:17 daily	**bpm_pmc_collect_24hr** cron	User: **bpm** Bulk Performance Monitoring (BPM) 24 hour data collection (retry).
05:32 6 hourly	**fm_log_suppressed** cron	User: **oms** Collection of suppressed alarm and TCA files from NAs and entering of them into the alarm history log.
05:47 daily	**bpm_pmc_collect_24h** cron	User: **bpm** Bulk Performance Monitoring (BPM) 24 hour data collection (retry).
* The full name of the cron job is the following: <*name*>*_cron.*<*user*>		

A note about PM data collection times

The default PM data collection times that are displayed in the "Table of scheduled activities" (p. 41-4) were selected to suit situations in which the network time and the server time are within two hours of each other, which is one of the following:

- NETWORK_TZ is set to SERVER_TIME
- NETWORK_TZ is set to UTC and the local time zone is the following:
  GMT, GMT+1, or GMT+2
  For example: central European time with daylight saving.

For other situations, administrators should consider modifying crontab so that the following occur:

- **bpm_pmc_collect_24h** is always after UTC midnight.
  Note: Coordinated Universal Time (UTC) is the international time standard. It is the current term for what was commonly referred to as *Greenwich Meridian Time (GMT)*.
- PM data collection should not be started in the hour preceding UTC midnight because it might result in the collection straddling the day boundary.
- If possible, these collection times should avoid the period of main user activity so the users do not experience slower system responses.

42 Platform Alarms

Overview

Purpose

This chapter explains platform alarms, which are those alarms that are generated internally by the management system.

Contents

Alarm Classifications

Service Affecting

In the broadest sense, alarms are classified as *service-affecting alarms* or *non-service affecting alarms*. As the terms suggest, service affecting alarms disrupt service to the management system users. Non-service affecting alarms do not disrupt service to management system users.

Severity Level

The management system classifies alarms by their severity level. Different names may be used to denote most of the same severity levels in systems that support the X.733 standard and the Prompt/Deferred/Information (PDI) standard. For example: the lowest alarm severity level in the X.733 standard is designated as a *warning*; the lowest alarm severity level in the PDI standard is designated as *information*.

For a further explanation of these severity levels, refer to the *OMS Service Assurance Guide*. For a list of alarms in each severity level, refer to the following table.

Severity Level	Alarm Name and Hot Link to Alarm Description
Warning/Information	"ALARMS_LOG_SPACE_LOW" (p. 42-7) "BACKUP_DATABASE_NOW" (p. 42-8) "CR_FULL" (p. 42-9) "CR_NEARLY_FULL" (p. 42-10) "CURRENT_ALARM_SPACE_LOW" (p. 42-10) "INVALID_PASSWD_DETECTED" (p. 42-18) "LOG_FILES_HAVE_BEEN_TRIMMED" (p. 42-19) "NEL_FULL" (p. 42-21) "NEL_NEARLY_FULL" (p. 42-22) "SL_FULL" (p. 42-25) "SL_NEARLY_FULL" (p. 42-26) "UTL_FULL" (p. 42-27) "UTL_NEARLY_FULL" (p. 42-27) "FLAPPING_ALARMS_DETECTED" (p. 42-16)
Minor/Deferred	"ALARMS_LOG_PURGE" (p. 42-7) "ALARMS_LOG_SPACE_VERY_LOW" (p. 42-8) "ALARMS_SUPPRESSED" (p. 42-8) "BACKUP_ERROR" (p. 42-9) "CURRENT_ALARM_SPACE_VERY_LOW" (p. 42-11) "DET_PUSH_FAILED" (p. 42-11) "EXCESSIVE_UNACKED_ALARMS" (p. 42-15) "EXCESSIVE_UNACKED_TCAS" (p. 42-16) "FS_INODES_WARNING" (p. 42-17) "FS_SPACE_WARNING" (p. 42-18) "FS_SPACE_WARNING" (p. 42-18) "NBI_SESSION_LOGOUT" (p. 42-20) "NE_LICENSE_EXCEEDED" (p. 42-21) "POST_NE_UPD_REQUIRED" (p. 42-25)

Severity Level	Alarm Name and Hot Link to Alarm Description
Major/Prompt	"BPM_15M_DATA_PURGED" (p. 42-9)
	"BPM_24H_DATA_PURGED" (p. 42-9)
	"DISK_STALE_PE" (p. 42-12)
	"DR_ACTSECTOPRI" (p. 42-12)
	"DR_PRITOACTSEC" (p. 42-13)
	"DR_PRITOSEC" (p. 42-13)
	"DR_RESYNC_PAUSED" (p. 42-12)
	"DR_RESYNC_STARTED" (p. 42-12)
	"DR_RESYNC_STOPPED" (p. 42-13)
	"DR_RLK_CONNECT" (p. 42-14)
	"DR_SECTOPRI" (p. 42-13)
	"DR_SRL_OVERFLOW" (p. 42-14)
	"DR_SRL_WARN" (p. 42-14)
	"ETHER_COLLISION" (p. 42-15)
	"ETHER_ERROR" (p. 42-15)
	"FM_RESTART" (p. 42-16)
	"FS_SPACE_LOW" (p. 42-17)
	"HA_COMMUNICATION_FAIL" (p. 42-18)
	"FS_INODES_LOW" (p. 42-16)
	"LO_UPGRADE_REQUIRED" (p. 42-19)
	"NE_ASSOC_LOST" (p. 42-21)
	"ONNS_ASSOC_LOST" (p. 42-22)
	"PID_DATA_SIZE" (p. 42-22)
	"PID_DEACTIVATED" (p. 42-23)
	"PID_STACK_SIZE" (p. 42-23)
	"PM_15M_DATA_PURGED" (p. 42-23)
	"PM_15M_RETENTION_LOW" (p. 42-24)
	"PM_24H_DATA_PURGED" (p. 42-24)
	"PM_24H_RETENTION_LOW" (p. 42-24)
	"PM_MONITORING_DISABLED" (p. 42-24)
	"PSE_LOG_PURGED" (p. 42-25)
	"SWAP_LOW_WARNING" (p. 42-26)
	"TCA_LOG_PURGED" (p. 42-26)
	"VCG_RESYNC_FAILED" (p. 42-27)
	"MRP_COMMS_DEACTIVATED" (p. 42-19)

Severity Level	Alarm Name and Hot Link to Alarm Description
Critical/Prompt	"CURRENT_ALARMS_SPACE_FULL" (p. 42-11) "FS_UNMOUNTED" (p. 42-18) "NA_ASSOC_LOST" (p. 42-20) "NA_COMMS_ERROR" (p. 42-20)

Component/Subsystem Type

The management system classifies alarms, and thus names alarms, according to the component/subsystem that generated the alarm. For example: alarms that are generated for Disaster Recovery configurations are prefaced with *DR*; alarms that are generated due to backup problems are prefaced with *BACKUP*.

The following table lists alarms that are generated by a particular component.

Component	Alarm
Alarm Log and Purging	"ALARMS_LOG_PURGE" (p. 42-7) "ALARMS_LOG_SPACE_LOW" (p. 42-7) "ALARMS_LOG_SPACE_VERY_LOW" (p. 42-8) "ALARMS_SUPPRESSED" (p. 42-8) "LOG_FILES_HAVE_BEEN_TRIMMED" (p. 42-19) "FLAPPING_ALARMS_DETECTED" (p. 42-16)
Alarm List and Purging	"CURRENT_ALARM_SPACE_LOW" (p. 42-10) "CURRENT_ALARMS_SPACE_FULL" (p. 42-11) "EXCESSIVE_UNACKED_ALARMS" (p. 42-15)
Backups	"BACKUP_DATABASE_NOW" (p. 42-8) "BACKUP_ERROR" (p. 42-9)
Bulk Performance Monitoring (BPM)	"BPM_15M_DATA_PURGED" (p. 42-9) "BPM_24H_DATA_PURGED" (p. 42-9)
Command Response (CR) Log	"CR_FULL" (p. 42-9) "CR_NEARLY_FULL" (p. 42-10) "LOG_FILES_HAVE_BEEN_TRIMMED" (p. 42-19)
Data Extraction Tool (DET)	"DET_PUSH_FAILED" (p. 42-11)

Component	Alarm
Disaster Recovery	“DR_ACTSECTOPRI” (p. 42-12) “DR_PRITOACTSEC” (p. 42-13) “DR_PRITOSEC” (p. 42-13) “DR_RESYNC_PAUSED” (p. 42-12) “DR_RESYNC_STARTED” (p. 42-12) “DR_RESYNC_STOPPED” (p. 42-13) “DR_RLK_CONNECT” (p. 42-14) “DR_SECTOPRI” (p. 42-13) “DR_SRL_OVERFLOW” (p. 42-14) “DR_SRL_WARN” (p. 42-14) “DR_ACTSECTOPRI” (p. 42-12) “DR_PRITOACTSEC” (p. 42-13) “DR_PRITOSEC” (p. 42-13) “DR_RESYNC_PAUSED” (p. 42-12) “DR_RESYNC_STARTED” (p. 42-12) “DR_RESYNC_STOPPED” (p. 42-13) “DR_RLK_CONNECT” (p. 42-14) “DR_SECTOPRI” (p. 42-13) “DR_SRL_OVERFLOW” (p. 42-14) “DR_SRL_WARN” (p. 42-14)
File System (FS)	“FS_INODES_LOW” (p. 42-16) “FS_INODES_WARNING” (p. 42-17) “FS_SPACE_LOW” (p. 42-17) “FS_SPACE_WARNING” (p. 42-18) “FS_UNMOUNTED” (p. 42-18)
High Availability (HA)	“HA_COMMUNICATION_FAIL” (p. 42-18)
LAN Monitoring	“ETHER_COLLISION” (p. 42-15) “ETHER_ERROR” (p. 42-15)
Licenses	“NE_LICENSE_EXCEEDED” (p. 42-21)

Component	Alarm
Lost Associations or Communications	“HA_COMMUNICATION_FAIL” (p. 42-18) “NA_ASSOC_LOST” (p. 42-20) “NA_COMMS_ERROR” (p. 42-20) “NBI_SESSION_LOGOUT” (p. 42-20) “ONNS_ASSOC_LOST” (p. 42-22)
Multi-Regional Provisioning (MRP)	“MRP_COMMS_DEACTIVATED” (p. 42-19)
Network Adapters (NAs)	“NA_ASSOC_LOST” (p. 42-20) “NA_COMMS_ERROR” (p. 42-20)
Network Elements (NEs)	“LO_UPGRADE_REQUIRED” (p. 42-19) “NE_ASSOC_LOST” (p. 42-21) “NE_LICENSE_EXCEEDED” (p. 42-21) “POST_NE_UPD_REQUIRED” (p. 42-25)
Notification Log (NEL)	“NEL_FULL” (p. 42-21) “NEL_NEARLY_FULL” (p. 42-22)
Performance Monitoring (PM)	“BPM_15M_DATA_PURGED” (p. 42-9) “BPM_24H_DATA_PURGED” (p. 42-9) “PM_15M_DATA_PURGED” (p. 42-23) “PM_15M_RETENTION_LOW” (p. 42-24) “PM_24H_DATA_PURGED” (p. 42-24) “PM_24H_RETENTION_LOW” (p. 42-24) “PM_MONITORING_DISABLED” (p. 42-24)
Process ID (PID)	“PID_DATA_SIZE” (p. 42-22) “PID_DEACTIVATED” (p. 42-23) “PID_STACK_SIZE” (p. 42-23)
Protection Switch Event (PSE) Log	“PSE_LOG_PURGED” (p. 42-25)
Security/Security Log (SL)	“INVALID_PASSWD_DETECTED” (p. 42-18) “SL_FULL” (p. 42-25) “SL_NEARLY_FULL” (p. 42-26)
System Hardware	“DISK_STALE_PE” (p. 42-12) “SWAP_LOW_WARNING” (p. 42-26)

Component	Alarm
Threshold Crossing Alert (TCA) Log	"EXCESSIVE_UNACKED_TCAS" (p. 42-16) "TCA_LOG_PURGED" (p. 42-26)
Users/User Activity Log	"INVALID_PASSWD_DETECTED" (p. 42-18) "UTL_FULL" (p. 42-27) "UTL_NEARLY_FULL" (p. 42-27)
Virtual Concatenation Group (VCG)	"VCG_RESYNC_FAILED" (p. 42-27)

List of Platform Alarms

ALARMS_LOG_PURGE

Alarm Text: The alarms log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, minor alarm.

Probable Cause: The Alarms Log storage space is full.

Recommended Action: Action is automatic. At storage capacity, a number of the oldest records stored in the Alarms Log are deleted. Archiving does not occur. The capacity and number of records to delete is set at installation time. If this alarm is raised regularly, reduce the retention period for the alarm log reduced by editing the installation parameters.

Related Information: The *OMS Service Assurance Guide*.

ALARMS_LOG_SPACE_LOW

Alarm Text: Historic alarm storage 80% full, recommend archive and delete from alarm log. On reaching capacity the alarm log shall be purged of a number of records.

Alarm Particulars: A non-service affecting, persistent, warning/information alarm.

Probable Cause: The Alarms Log is becoming full. The alarms stored in the management system Alarms Log exceed 80% of the configured limit, which is set during system installation.

Recommended Action: Archive alarms and manually delete them from the history list. The extent of how many alarms you delete depends on your maintenance strategies; for example, deleting all cleared alarms that have been in the history list for a certain period of time should be done as part of routine maintenance. Warning: when the storage space reaches 95% of the configured value, periodic purges automatically occur to reduce the size of the Alarms Log by 10%.

Related Information: “Log Concepts” (p. 13-1) and the *OMS Service Assurance Guide*.

ALARMS_LOG_SPACE_VERY_LOW

Alarm Text: Historic alarm storage 95% full, oldest 10% of records deleted from alarm log.

Alarm Particulars: A non-service affecting, persistent, minor/deferred alarm.

Probable Cause: The Alarms Log storage space is 95% full. The absolute limit is set during the installation of the system.

Recommended Action: The management system action is automatic. When 95% of the storage capacity becomes full, the oldest 10% of records stored in the Alarms Log are automatically deleted. Archiving does not occur.

Related Information: “Log Concepts” (p. 13-1) and the *OMS Service Assurance Guide*.

ALARMS_SUPPRESSED

Alarm Text: Suppressed Alarms Detected.

Alarm Particulars: A non-service affecting, transient, minor alarm.

Probable Cause: New suppressed alarms have been placed in the log.

Recommended Action: Check the alarms added to the alarm log on the same day in which the alarm was raised. Search for short duration alarms (those that are less than the current alarm raise hold-off time) and/or those with the **Make historic user** shown as **Suppressed**.

Related Information: Refer to the OMS Service Assurance Guide for additional information regarding alarms and alarm suppression.

Note: The ALARMS_SUPPRESSED alarm can be disabled, refer to “Suppressed Alarms Logging” (p. 6-28) for more details.

BACKUP_DATABASE_NOW

Alarm Text: Archived database file(s) removed, backup the database immediately.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: More than 80% of the **<DB backup directory>** file system has been consumed, which resulted in older database archives being removed by routine housekeeping.

Recommended Action: Backup the database.

Related Information: “System Backups” (p. 10-2), “Execute an Immediate Hot System Backup from the OMS” (p. 10-8), and “Execute a Cold System Backup from the HP® Server” (p. 10-9).

BACKUP_ERROR

Alarm Text: Backup failed, unknown cause.

Alarm Particulars: A non-service affecting, transient, minor/deferred alarm

Probable Cause: The backup failed and the cause is not known.

Recommended Action: Check the console log messages or contact Alcatel-Lucent Customer Support Services.

Related Information: "Log Concepts" (p. 13-1) and "System Backups" (p. 10-2). Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

BPM_15M_DATA_PURGED

Alarm Text: 15 Min History Data has been Purged from the System.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The network generated too much 15-minute data to be stored in the management system.

Recommended Action: Contact Alcatel-Lucent Customer Support Services if the problem frequently re-occurs.

Related Information: "BPM" (p. 11-6) and refer to the *OMS Service Assurance Guide* for more information about performance monitoring. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

BPM_24H_DATA_PURGED

Alarm Text: 24 Hour History Data has been Purged from the System.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The network generated too much 24-hour data to be stored in the management system.

Recommended Action: Contact Alcatel-Lucent Customer Support Services if the problem frequently re-occurs.

Related Information: "BPM" (p. 11-6) and refer to the *OMS Service Assurance Guide* for more information about performance monitoring. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

CR_FULL

Alarm Text: The command and response log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The command response log has become full and has now deleted 25% of its oldest records.

Recommended Action: Archive or print records first; then delete records from the command response log to avoid the reoccurrence of this alarm.

Related Information: "Log Concepts" (p. 13-1); the "Enable Command Response Log" (p. 6-15), and the "Command Response Log Retention Time Period" (p. 6-15) installation parameters; and the *OMS Network Element Management Guide*.

CR_NEARLY_FULL

Alarm Text: Command Response log has exceeded 80% full threshold.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The command response log is more than 80% full.

Recommended Action: Archive or print records first; then delete records from the log. (The log automatically deletes old records if it becomes full.)

Related Information: "Log Concepts" (p. 13-1); the "Enable Command Response Log" (p. 6-15), and the "Command Response Log Retention Time Period" (p. 6-15) installation parameters; and the *OMS Network Element Management Guide*.

CURRENT_ALARM_SPACE_LOW

Alarm Text: The number of current alarms has exceeded 80% of the configured record limit. Automatic deletion of records will take place at and above 95%. It is recommended that you take action now to reduce the number of current alarms in the Alarms List.

Alarm Classification: A non-service affecting, persistent, warning/information alarm.

Probable Cause: The current alarm list is becoming very full. The alarms stored in the current alarm list of the management system exceed 80% of the configured limit. This limit is set during the installation of the system.

Recommended Action: Acknowledge cleared alarms so they are removed from the current Alarms List. To free up space, delete instantaneous alarms that are no longer required. The extent of how many alarms you delete depends on your maintenance strategies; for example, deleting all cleared alarms that have been in the current alarm list for a certain period of time should be done as part of routine maintenance. Warning: when the storage space reaches 95% of the configured value, periodic purges automatically occur to reduce the size of the Alarms List by 10%.

Related Information: The "FM Instantaneous Alarm Delete Age" (p. 6-17) installation parameter and the *OMS Service Assurance Guide*.

CURRENT_ALARM_SPACE_VERY_LOW

Alarm Text: Alarms List is over 95% full. Periodic purges to reduce Alarm List by 10% now taking place until below 95%. It is recommended that you take further action now to reduce the number of alarms below 80% and/or contact LWS for support.

Alarm Classification: A non-service affecting, persistent, major alarm.

Probable Cause: The current alarm list is becoming very full. The alarms stored in the management system's current alarm list exceeds 95% of the configured limit. This limit is set at installation.

Recommended Action: Periodic attempts are automatically made to reduce the number of current alarms by 10% of the configured record limit until the number of current alarms in the Alarms List is below 95% . When the number of current alarms is below 95%, this alarm will be cleared. Purging is done by deleting cleared persistent alarms and then deleting instantaneous alarms over 7 days old. Take further action now to reduce the number of alarms below 80%. If this alarm occurring regularly, contact Alcatel-Lucent Customer Support Services to investigate increasing the configured size of the Alarms List.

Related Information: The "FM Instantaneous Alarm Delete Age" (p. 6-17) installation parameter and the *OMS Service Assurance Guide*. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

CURRENT_ALARMS_SPACE_FULL

Alarm Text: The current alarm list is full

Alarm Classification: A service affecting, persistent, critical alarm.

Probable Cause: The current alarm list is full and OMS has been unable to purge any entries

Recommended Action: Take action immediately to reduce the number of alarms below 95% and/or contact Alcatel-Lucent Customer Support Services for support. Failure to take action can adversely affect system performance and stability.

Related Information: The *OMS Service Assurance Guide*. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

DET_PUSH_FAILED

Alarm Text: Data Extraction couldn't copy a file to a remote system.

Alarm Particulars: A non-service affecting, transient, minor/deferred alarm.

Probable Cause: The Data Extraction tool could not copy the specified file to the remote system. See the DET log for more details.

Recommended Action: Check the DET log. Contact the administrator of the remote system.

Related Information: Chapter 16, “Data Extraction”.

DISK_STALE_PE

Alarm Text: A physical volume has stale physical extents.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: Heavy disk I/O or failed disk.

Recommended Action: Run **vxdisk list** to get a list of your disks; then, run **vxdisk list <disk name>** for the status of a particular disk. If the figures displayed for *Stale PE* do not decrease over time, contact Alcatel-Lucent Customer Support Services.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

DR_ACTSECTOPRI

Alarm Text: VERITAS detects switch from acting standby to active.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. ACTSECTOPRI signifies *active secondary to primary* .

Probable Cause: The system role switched from acting standby to active.

Recommended Action: Informational only.

Related Information: “Disaster Recovery Concepts” (p. 20-2).

DR_RESYNC_PAUSED

Alarm Text: VERITAS Replication Volume Group Resync Paused.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. RESYNC signifies *resynchronization*.

Probable Cause: Operator interference has occurred; the link between the active and the standby is down; or the standby system is down.

Recommended Action: Resume resynchronization as soon as possible.

Related Information: “Disaster Recovery Concepts” (p. 20-2).

DR_RESYNC_STARTED

Alarm Text: VERITAS Replication Volume Group Resync Started.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. RESYNC signifies *resynchronization*.

Probable Cause: Operator interference has occurred; or the resynchronization can occur automatically if the link between the active and standby systems is restored or the standby has come back up.

Recommended Action: Do nothing; this alarm is information.

Related Information: "Disaster Recovery Concepts" (p. 20-2).

DR_RESYNC_STOPPED

Alarm Text: VERITAS Replication Volume Group Resync Stopped.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. RESYNC signifies *resynchronization*.

Probable Cause: Operator interference has occurred; the link between the active and standby systems is down; or the standby system is down.

Recommended Action: Restart resynchronization as soon as possible.

Related Information: "Disaster Recovery Concepts" (p. 20-2) and the *OMS Network Element Management Guide* and/or the *OMS Ethernet Management Guide*.

DR_PRITOACTSEC

Alarm Text: VERITAS detects switch from active to acting standby.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. PRITOACTSEC signifies *primary to acting secondary*.

Probable Cause: The system role switched from active to acting standby.

Recommended Action: Informational only.

Related Information: "Disaster Recovery Concepts" (p. 20-2).

DR_PRITOSEC

Alarm Text: VERITAS detects switch from active to standby.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. PRITOSEC signifies *primary to secondary*.

Probable Cause: The system role switched from active to standby.

Recommended Action: Informational only.

Related Information: "Disaster Recovery Concepts" (p. 20-2).

DR_SECTOPRI

Alarm Text: VERITAS detects switch from standby to active.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. SECTOPRI signifies *secondary to primary* .

Probable Cause: The system role switched from standby to active.

Recommended Action: Informational only.

Related Information: "Disaster Recovery Concepts" (p. 20-2).

DR_RLK_CONNECT

Alarm Text: VERITAS Replication Link is down.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. RLK signifies *Replication Link*.

Probable Cause: The link between the active and standby systems is down; or the standby system is down.

Recommended Action: Check the standby system. Check the communication links between the active and standby systems.

Related Information: "Disaster Recovery Concepts" (p. 20-2).

DR_SRL_OVERFLOW

Alarm Text: VERITAS Storage Replication Log is Full. DCM Logging has begun.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. SRL signifies *Storage Replication Log*. DCM signifies *Data Change Map*.

Probable Cause: The machine is heavily loaded; the link between active and standby systems is down; or, the standby system is down.

Recommended Action: Check the standby system. Check the communication links between the active and standby systems. Resolve the problems immediately, or you might have to perform a full resynchronization. See the "Resynchronize the Active System after an SRL Overflow" (p. 20-24) task. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: "Disaster Recovery Concepts" (p. 20-2) , the "Resynchronize the Active System after an SRL Overflow" (p. 20-24) task, and the *OMS Network Element Management Guide*. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

DR_SRL_WARN

Alarm Text: VERITAS Storage Replication Log is 80% Full.

Alarm Particulars: A service affecting, transient, major/prompt alarm. DR signifies a *Disaster Recovery* configuration. SRL signifies *Storage Replication Log*.

Probable Cause: The machine is heavily loaded; the link between active and standby is down; or the standby is down.

Recommended Action: Check the standby system. Check the communication links between the active and standby systems. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: "Disaster Recovery Concepts" (p. 20-2). Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

ETHER_COLLISION

Alarm Text: A LAN interface is reporting Ethernet collisions.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: An Ethernet cabling insulation fault exists or the network load is high.

Recommended Action: Check the Ethernet cabling and the network load. Hint: use the UNIX® **lanadmin** command to check Ethernet statistics. In addition, for the HP® server on which the management system resides, refer to the Chapter 12, "Resource Monitor" for details on monitoring LAN errors.

ETHER_ERROR

Alarm Text: A LAN interface is reporting Ethernet errors.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: The Ethernet connection has been severed; a cabling insulation fault exists; or the network load is high.

Recommended Action: Check the Ethernet connection, the cabling, and the network load. Hint: use the UNIX® **lanadmin** command to check Ethernet statistics. In addition, for the HP® server on which the management system resides, refer to the Chapter 12, "Resource Monitor" for details on monitoring LAN errors.

EXCESSIVE_UNACKED_ALARMS

Alarm Text: There are too many unacknowledged alarms.

Alarm Particulars: A non-service affecting, persistent, minor alarm.

Probable Cause: The Alarms List is more than 60% full.

Recommended Action: Acknowledge some of the alarms or change the alarm acknowledgement setting in the management system. If action is not taken, the management system will encounter performance problems.

Related Information: The *OMS Service Assurance Guide*.

EXCESSIVE_UNACKED_TCAS

Alarm Text: There are too many unacknowledged TCAs.

Alarm Particulars: A non-service affecting, persistent, minor alarm.

Probable Cause: The TCA list contains too many threshold crossing alerts (TCAs) that are not being placed in the historic state because they have not been acknowledged.

Recommended Action: Acknowledge some of the alarms or change the alarm acknowledgement setting in the management system. If action is not taken, the management system will encounter performance problems.

Related Information: The *OMS Service Assurance Guide*.

FLAPPING_ALARMS_DETECTED

Alarm Text: Flapping alarms on NE %s.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The number of instances of a particular alarm compared to an individual port on an NE exceeds the threshold.

Recommended Action: Check the alarm list and alarm log for flapping alarms and then investigate the cause of those alarms.

Related Information: "Log Concepts" (p. 13-1) and the *OMS Service Assurance Guide*.

FM_RESTART

Alarm Text: Fault Management Component Restarted.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The Fault Management Component has been restarted.

Recommended Action: Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

FS_INODES_LOW

Alarm Text: Indicated file system is running very low on available inodes.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. An FS is a file system.

Probable Cause: Each file within a file system has an associated inode. A file system is automatically allocated a quota of inodes when it is created. The more files that exist in a file system, the more inodes that will be used.

Recommended Action: Backup the system immediately. Use the UNIX® **bdf** command to determine file system usage. Delete redundant files. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

FS_INODES_WARNING

Alarm Text: Indicated file system is running low on available inodes.

Alarm Particulars: A non-service affecting, persistent, minor alarm. An FS is a file system.

Probable Cause: Each file within a file system has an associated inode. A file system is automatically allocated a quota of inodes when it is created. The more files that exist in a file system, the more inodes that will be used.

Recommended Action: Schedule a system backup at the earliest convenient time. Use the UNIX® **bdf** command to determine file system usage. Delete redundant files. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

FS_SPACE_LOW

Alarm Text: File system %s is running very low on available space.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. An FS is a file system.

Probable Cause: Large core files, redundant temporary files, and/or archive and log files exist. The file system usage is inappropriate (for example, the temporary storage area).

Recommended Action: Backup the system immediately. Use the UNIX® **bdf** command to determine file system usage. Delete redundant files. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

FS_SPACE_WARNING

Alarm Text: File system %s is running low on available space.

Alarm Particulars: A non-service affecting, persistent, minor/deferred alarm. An FS is a file system.

Probable Cause: Large core files, redundant temporary files, and/or archive and log files exist. The file system usage is inappropriate (for example, the temporary storage area).

Recommended Action: Schedule a system backup at the earliest convenient time. Use the UNIX® **bdf** command to determine file system usage. Delete redundant files. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

FS_UNMOUNTED

Alarm Text: File system %s has become unmounted.

Alarm Particulars: A service affecting, persistent, critical/prompt alarm. An FS is a file system.

Probable Cause: A hardware failure has occurred.

Recommended Action: Contact Alcatel-Lucent Customer Support Services immediately.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

HA_COMMUNICATION_FAIL

Alarm Text: HA: Communication failure with remote OMS. **Alarm Text:** A user has made multiple unsuccessful attempts to login.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The OMS has been unable to communicate with the other OMS system.

Recommended Action: Check the connection between the OMS system pair and restart the session.

Related Information: "Start the Platform" (p. 9-5).

INVALID_PASSWD_DETECTED

Alarm Text: A user has made multiple unsuccessful attempts to login.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: A user has made a series of attempts to login into the management system using an invalid password. The users account may now be locked.

Recommended Action: Check the user transaction log for details, such as the user name. Check with the particular user. If the user accidentally made an error, unlock the user's account through the administration interface. If you have determined that the user did not accidentally make an error, alert security personnel.

Related Information: "Log Concepts" (p. 13-1); "User ID Rules" (p. 8-9); "Password Rules" (p. 8-11); the"Password Aging Time" (p. 6-121), the "Password Warning Time" (p. 6-122), and the "Password Period of Non Use" (p. 6-122) installation parameters; and the *OMS Network Element Management Guide*.

LOG_FILES_HAVE_BEEN_TRIMMED

Alarm Text: Older log files have been automatically removed.

Alarm Particulars: A non-service affecting, transient warning/information alarm.

Probable Cause: More than 80% of the **<log directory>** file system has been consumed, which has resulted in the automatic removal of some older log files.

Recommended Action: Immediate action not required. If the condition persists, Contact Alcatel-Lucent Customer Support Services.

Related Information: "Log Concepts" (p. 13-1). Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

LO_UPGRADE_REQUIRED

Alarm Text: LambdaUnite Requires Upgrading to Support LO XC.

Alarm Particulars: A non-service affecting, persistent major/prompt alarm.

Probable Cause: A circuit pack that supports low-order cross connections has been installed.

Recommended Action: Run the OmsInServiceUpgrade tool.

Related Information: "NE In-Service Upgrade Concepts" (p. 25-1); and specifically the "Run the NE In-Service Upgrade Tool from the Command Line" (p. 25-4) task.

MRP_COMMS_DEACTIVATED

Alarm Text: The communication with MRP has been Deactivated.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: A user has deactivated the communications link with MRP.

Recommended Action: No VCG updates will be performed until the communications link is re-activated. This can be performed from the Controller List page.

Related Information: Refer to Optical PM-MRP Guide for more information. And Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

NA_ASSOC_LOST

Alarm Text: Association with a Network Adaptor lost.

Alarm Particulars: A service affecting, persistent, critical/prompt alarm.

Probable Cause: The communication link between the network adapter (NA) and this system might have failed; or, the network adapter might have released communication or is not running.

Recommended Action: Check the links between the management system and the NA. If the links are fine, restart the NA application. If the problem still exists, restart the management system application. If the problem persists, contact Alcatel-Lucent Customer Support Services.

Related Information: “Start the Platform” (p. 9-5). Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

NA_COMMS_ERROR

Alarm Text: Network Adaptor Comms error.

Alarm Particulars: A service affecting, transient, critical/prompt alarm.

Probable Cause: The network adapter (NA) and the management system have a connection; but, they cannot establish communication across the connection.

Recommended Action: Contact Alcatel-Lucent Customer Support Services.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

NBI_SESSION_LOGOUT

Alarm Text: Terminated Session on the Northbound Client.

Alarm Particulars: A service affecting, transient, minor/deferred alarm. An NBI is a northbound interface.

Probable Cause: The session of a northbound client was terminated because the northbound client did not respond to the management system.

Recommended Action: Check the connection between the management system and the northbound client; restart the session from the northbound client.

NE_ASSOC_LOST

Alarm Text: Association with an NE lost.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. An NE is a network element.

Probable Cause: Numerous probable causes exist for this alarm, such as the failure of a card or the LAN interface, the removal or severance of one or more optical fibers, the removal of LAN terminating impedance, or the installation of additional equipment on a shared LAN.

In addition, this alarm can be raised due to a misconfigured DCN that causes stability problems between a management system CMISE network adapter (CNA) and any CMISE NE. Specifically, the problem occurs when the duplex mode and the rate differ between the CNA and the NE, the CNA and an intermediate router, or a router and the NE.

Recommended Action: Identify the problem and rectify it. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

NE_LICENSE_EXCEEDED

Alarm Text: The number of NEs allowed by the stated license have been exceeded.

Alarm Particulars: Non-service affecting, transient, minor/deferred alarm. An NE is a network element.

Probable Cause: An NE of the specified type has been added to the system and the licenses available are insufficient to handle this NE type.

Recommended Action: Contact Alcatel-Lucent Customer Support Services to obtain more NE licenses.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

NEL_FULL

Alarm Text: The NE notification log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The notification log has become full and has now deleted 25% of its oldest records.

Recommended Action: Archive or print records first; then delete records from the notification log to avoid the reoccurrence of this alarm.

Related Information: "Log Concepts" (p. 13-1); the "Enable NE Notification Log" (p. 6-14), and the "NE Notification Log Retention Time Period" (p. 6-14) installation parameters; the "NEL_NEARLY_FULL" (p. 42-22) platform alarm; and the *OMS Network Element Management Guide*.

NEL_NEARLY_FULL

Alarm Text: Notification log has exceeded 80% full threshold.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The notification log is more than 80% full.

Recommended Action: Archive or print records first; then delete records from the log. (The log automatically deletes old records if it becomes full.)

Related Information: "Log Concepts" (p. 13-1); the "Enable NE Notification Log" (p. 6-14), and the "NE Notification Log Retention Time Period" (p. 6-14) installation parameters; the "NEL_FULL" (p. 42-21) platform alarm; and the *OMS Network Element Management Guide*.

ONNS_ASSOC_LOST

Alarm Text: Association with an ONNS lost.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. An ONNS is an Optical Network Navigation System.

Probable Cause: Numerous probable causes exist for this alarm, such as the failure of a card or the LAN interface, the removal or severance of one or more optical fibers, the removal of LAN terminating impedance, or the installation of additional equipment on a shared LAN.

Recommended Action: Identify the problem and rectify it. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: "Enable ONNS Feature" (p. 6-89) and "FM ONNS Reroute Display" (p. 6-20) installation parameters. Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

PID_DATA_SIZE

Alarm Text: A PID's data segment is near the maximum size.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. A PID is a process ID.

Probable Cause: A process is heavily loaded.

Recommended Action: If possible, restart the application; otherwise, schedule a reboot. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

PID_DEACTIVATED

Alarm Text: A PID has been deactivated.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. PID is a process ID.

Probable Cause: The machine is heavily loaded and a high level of swapping has occurred.

Recommended Action: Schedule a reboot. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

PID_STACK_SIZE

Alarm Text: A PID's stack segment is near the maximum.

Alarm Particulars: A service affecting, persistent, major/prompt alarm. A PID is a process ID.

Probable Cause: A process is heavily loaded.

Recommended Action: If possible, restart the application; otherwise, schedule a reboot. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

PM_15M_DATA_PURGED

Alarm Text: 15 Min History Data has been Purged from the System.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The number of termination points (TPs) that are being monitored are greater than that which is allowed to maintain the requested 15 minute retention period.

Recommended Action: Disable the monitoring of TPs, clear the data for TPs, or reduce the configured retention time.

Related Information: Refer to the *OMS Service Assurance Guide* for more information about performance monitoring.

PM_15M_RETENTION_LOW

Alarm Text: 15 Min History Data Retention has fallen below limit.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: The number of termination points (TPs) that are being monitored are greater than that which is allowed to maintain the requested 15 minute retention period.

Recommended Action: Disable the monitoring of TPs, clear the data for TPs, or reduce the configured retention time.

Related Information: Refer to the *OMS Service Assurance Guide* for more information about performance monitoring.

PM_24H_DATA_PURGED

Alarm Text: 24 Hour History Data has been Purged from the System.

Alarm Particulars: A service affecting, transient, major/prompt alarm.

Probable Cause: The number of termination points (TPs) that are being monitored are greater than that which is allowed to maintain the requested 24 hour retention period.

Recommended Action: Disable the monitoring of TPs, clear the data for TPs, or reduce the configured retention time.

Related Information: Refer to the *OMS Service Assurance Guide* for more information about performance monitoring.

PM_24H_RETENTION_LOW

Alarm Text: 24 Hour History Data Retention has fallen below limit.

Alarm Particulars: A non-service affecting, persistent, major/prompt alarm.

Probable Cause: The number of termination points (TPs) that are being monitored are greater than that which is allowed to maintain the requested 24 hour retention period.

Recommended Action: Disable the monitoring of TPs, clear the data for TPs, or reduce the configured retention time.

Related Information: Refer to the *OMS Service Assurance Guide* for more information about performance monitoring.

PM_MONITORING_DISABLED

Alarm Text: Monitoring has been disabled for layer rate %s.

Alarm Particulars: A non-service affecting, transient, major/prompt alarm.

Probable Cause: PM data collection for a rate has been disabled because it could not be collected on a regular basis.

Recommended Action: Analyze the DCN topology to determine why all of the PM data cannot be collected.

Related Information: Refer to the *OMS Service Assurance Guide* for more information about performance monitoring.

POST_NE_UPD_REQUIRED

Alarm Text: Database Conversion Required after NE Upgrade.

Alarm Particulars: A non-service affecting, transient, minor alarm.

Probable Cause: The system has detected that the specified NE has been upgraded to a new release and a management system database conversion is required.

Recommended Action: Perform the database conversion with the OmsUpdateDatabase-For NE Upgrade.

Related Information: Refer to the *OMS Network Element Management Guide* for more information about NE Upgrade.

PSE_LOG_PURGED

Alarm Text: The PSE log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, major alarm.

Probable Cause: The Protection Switch Event (PSE) log exceeded its maximum size because too many PSEs were generated.

Recommended Action: If this problem persists, reduce the number of days that PSEs are being kept for by editing the "FM Protect Switch Log Retention Time" (p. 6-25) installation parameter.

Related Information: "FM Protect Switch Log Retention Time" (p. 6-25), "FM Enable Equipment Protection Switch Log" (p. 6-21), "FM Enable TDM MSP Protection Switch Log" (p. 6-22), "FM Enable MSSPRING Protection Switch Log" (p. 6-22), "FM Enable Non-Switch Protection Switch Log" (p. 6-23),"FM Enable TDM SNCP Protection Switch Log" (p. 6-23), "FM Enable WDM SNCP Protection Switch Log" (p. 6-24), and "FM Protect Switch Log Retention Time" (p. 6-25) installation parameters.

SL_FULL

Alarm Text: The security log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The security log has become full and has now deleted 25% of its oldest records.

Recommended Action: Archive or print records first; then delete records from the security log to avoid the reoccurrence of this alarm.

Related Information: "Log Concepts" (p. 13-1); the "Security Log user task" (p. 7-21); the "View a List of a Security Log Records" (p. 13-4) and the "View the Details of a Security Log Record" (p. 13-5) tasks; and the "Enable Security Log" (p. 6-12) installation parameters; and the "SL_NEARLY_FULL" (p. 42-26) platform alarm.

SL_NEARLY_FULL

Alarm Text: Security log has exceeded 80% full threshold.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The security log is more than 80% full.

Recommended Action: Archive or print records first; then delete records from the log. (The log automatically deletes old records if it becomes full.)

Related Information: "Log Concepts" (p. 13-1), the "Security Log user task" (p. 7-21), the "View a List of a Security Log Records" (p. 13-4) and the "View the Details of a Security Log Record" (p. 13-5) tasks, and the "Enable Security Log" (p. 6-12) installation parameters, and the "SL_FULL" (p. 42-25) platform alarm.

SWAP_LOW_WARNING

Alarm Text: The system is running very low on virtual memory.

Alarm Particulars: A service affecting, persistent, major/prompt alarm.

Probable Cause: Main system memory uses virtual memory as a temporary storage area. This alarm indicates an erroneous condition in which the system is becoming exhausted of all available memory.

Recommended Action: Reboot the system immediately. Contact Alcatel-Lucent Customer Support Services if the problem persists.

Related Information: Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

TCA_LOG_PURGED

Alarm Text: The TCA log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, major alarm.

Probable Cause: The Threshold Crossing Alert (TCA) log exceeded its maximum size because too many TCAs were generated.

Recommended Action: If this problem persists, reduce the number of days that TCAs are being kept for by editing the "FM TCA Log Retention Time" (p. 6-25) installation parameter.

Related Information: "FM TCA Log Retention Time" (p. 6-25) installation parameter.

UTL_FULL

Alarm Text: The user activity log has become full and the oldest records have been removed.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The user activity log has become full and has now deleted 25% of its oldest records.

Recommended Action: Archive or print records first; then delete records from the user log to avoid the reoccurrence of this alarm.

Related Information: "Log Concepts" (p. 13-1); "Connection Auto Discovery and the User Activity Log" (p. 22-3); the "Enable User Activity Log" (p. 6-13), and the "User Activity Log Retention Time Period" (p. 6-13) installation parameters; the "UTL_NEARLY_FULL" (p. 42-27) platform alarm; and the *OMS Network Element Management Guide*.

UTL_NEARLY_FULL

Alarm Text: User activity log has exceeded 80% full threshold.

Alarm Particulars: A non-service affecting, transient, warning/information alarm.

Probable Cause: The user activity log is more than 80% full.

Recommended Action: Archive or print records first; then delete records from the log. (The log automatically deletes old records if it becomes full.)

Related Information: "Log Concepts" (p. 13-1);"Connection Auto Discovery and the User Activity Log" (p. 22-3); the "Enable User Activity Log" (p. 6-13), and the "User Activity Log Retention Time Period" (p. 6-13) installation parameters; the "UTL_FULL" (p. 42-27) platform alarm; and the *OMS Network Element Management Guide*.

VCG_RESYNC_FAILED

Alarm Text: The VCG resync with MRP failed: %s.

Alarm Particulars: A non-service affecting, transient, major/prompt alarm.

Probable Cause: The VCG resynchronisation between EPM and MRP failed.

Recommended Action: If the problem persists, Contact Alcatel-Lucent Customer Support Services.

Related Information: Refer to *OMS Connection Management Guide*. And Alcatel-Lucent Customer Support Services can be reached at 866-582-3688 in the USA or 630-224-4672 outside the USA.

43 Special Operations

Overview

Purpose

This chapter contains conceptual information and the related tasks that are needed for the special operations that are involved with the management system.

Contents

Special Operations Concepts

Special operations definition

Special operations are those tasks that must be occasionally performed in relationship to a particular NE or to a particular group of NEs in order to ensure the proper functioning of the management system or the general network.

NE support for a particular release

Before executing any of the tasks that are in this chapter, refer to the "Summary of supported NEs" (p. 1-5) to determine if the particular NE or the particular group of NEs is supported in the current release of the management system.

Tasks related to special operations

The following tasks are related to special operations:

- "Restore the 1675 Lambda Unite MultiService Switch (MSS) Database from the Management System" (p. 43-3)
- "Set Up 1625 LambdaXtreme® Transport EPT Communication" (p. 43-5)
- "Retrieve a 1625 LambdaXtreme® Transport Database File from the HP® Server " (p. 43-7)
- "Insert an ONNS Node in an Active ONNS Network" (p. 43-9)
- "Replace Controller Units for CMISE NEs" (p. 43-11)

In addition, Chapter 4, "Cut Throughs" gives the conceptual information and the tasks that are needed to establish a cut-through to the 1675 Lambda Unite MultiService Switch (MSS) craft interface terminal (CIT).

Restore the 1675 Lambda Unite MultiService Switch (MSS) Database from the Management System

When to use

Use this task to restore the 1675 Lambda Unite MultiService Switch (MSS) database from the management system HP® server and to restore it manually using the 1675 Lambda Unite MultiService Switch (MSS) CIT.

Related information

See the following topic in this document:

- "Summary of supported NEs" (p. 1-5)

Before you begin

You must have a copy of the *1675 Lambda Unite MultiService Switch (MSS) User and Operations Guide* handy and you must follow the procedures documented for the database retrieval process and the database restoration process using the NE CIT. Note that this document is installed with the CIT.

The particular NE must be up and running and in full communication with its CIT.

The HP® server in which the management system resides must be up and running and must contain a backup of the 1675 Lambda Unite MultiService Switch (MSS) database.

This task requires the use of a file compression/decompression program such as *WinRar* or *WinZip* and it requires the use of a file transfer program such as *FTP* or *WS_FTP*.

You must have a working knowledge of the UNIX® OS and its commands.

Task

Use this task to backup the 1675 Lambda Unite MultiService Switch (MSS) database from the management system HP® server and to restore manually using the 1675 Lambda Unite MultiService Switch (MSS) CIT.

1 From the machine on which the management system is running, log in as **`oms`**.

2 Enter the following command to change directories to the directory containing the 1675 Lambda Unite MultiService Switch (MSS) database:

```
cd /var/opt/lucent/ftp/pub/obr/UNITE/<NE NAME>/<DATE>.<TIME>/
database files
```

Where:

<NE NAME> is the TID of the 1675 Lambda Unite MultiService Switch (MSS) to be restored.

<DATE>.<TIME> is the date and the time in which the backup using the management system was performed.

Example:

```
cd /var/opt/lucent/ftp/pub/obr/UNITE/NODE1/2005-01-31.18130:05/
<database files>
```

Result: The directory is changed as indicated.

---

3 Enter the following command line to **tar** the files:

```
tar -cvf /tmp/<mybackup files>.tar *
```

Result: The file is compressed.

---

4 Using a file transfer program, connect to the management system HP® server and **ftp**, in binary mode, the file **/tmp/<mybackup files>.tar** to a PC in which 1675 Lambda Unite MultiService Switch (MSS) CIT software is installed.

---

5 Uncompress the files that were moved over using whatever compression/decompression software is available on the CIT.

---

6 Use the *1675 Lambda Unite MultiService Switch (MSS) User and Operations Guide* and follow the procedures documented for the database restoration process using the NE CIT.

---

7 Log in to the management system and perform a full database synchronization for the NE that was restored to ensure that the management system and the NE are synchronized.

END OF STEPS

Set Up 1625 LambdaXtreme® Transport EPT Communication

When to use

Use this task to set up communication with the 1625 LambdaXtreme® Transport Engineering and Planning Tool (EPT).

Related information

See the following topic in this document:

- "OMS_NETINV license" (p. 5-12)
- "Stop the Platform" (p. 9-7)
- "Summary of supported NEs" (p. 1-5)

Before you begin

This task requires the "OMS_NETINV license" (p. 5-12) to be installed.

You need to have the IP address of the EPT server handy.

In addition, Step 1 of this task requires you to complete the "Stop the Platform" (p. 9-7) task.

Task

Use this task to set up communication with the Engineering and Planning Tool (EPT).

1 Complete the steps in the "Stop the Platform" (p. 9-7) task.

2 Enter the following command line to access the **cgw.properties** file:

```
vi /opt/lucent/oms/config/cgw.properties
```

3 Set the EPT properties as follows:

```
ept.present=true

ept.port=9622

ept.servername=<IP address of the EPT server>
```

4 Save the corrections that you have made to the file:

```
<Shift> ZZ
```

END OF STEPS

Retrieve a 1625 LambdaXtreme® Transport Database File from the HP® Server

When to use

Use this task to retrieve a 1625 LambdaXtreme® Transport database file from the HP® server on which the management system is running.

Related information

See the following topic in this document:

- "Summary of supported NEs" (p. 1-5)

Before you begin

This task requires the use of a file compression/decompression program such as WinRar or WinZip and it requires the use of a file transfer program such as FTP or WS_FTP.

Task

Use this task to retrieve a 1625 LambdaXtreme® Transport database file from the HP® server on which the management system is running.

1 From the machine on which the management system is running, log in as **`root`**.

2 Enter the following command to change directories to the directory containing the 1625 LambdaXtreme® Transport database:

```
cd /data/ftp/pub/obr/LX/<TID>/<date>.<time>
```

Where:

TID is the name of the 1625 LambdaXtreme® Transport NE in which the database is to be retrieved.

<date>.<time> is the actual date and the time in which the database is to be retrieved.

Result: The directory is changed as indicated.

3 Enter the following command to tar the files:

```
tar -cvf/tmp/<TIDbackup files>.tar*
```

4 Using a file transfer program, connect to the management system HP® server; and ftp, in binary mode, the file **tmp/<TIDbackup files>.tar*** to a PC in which 1625 LambdaXtreme® Transport CIT software is installed.

5 If the new Flash Memory Module is going to be build onsite, email the database files to a field technician.

END OF STEPS

Insert an ONNS Node in an Active ONNS Network

When to use

Along with the appropriate NE document, use this task to insert an Optical Network Navigator System (ONNS) node in an active ONNS Network.

> **Important!** This task addresses the behavior of OMS when the insert ONNS node procedure is followed and should be used in conjunction with the appropriate NE documentation. The exact procedure to insert an ONNS node in an active ONNS network is defined in the NE documentation.

Related information

See the following topic in this document:

- "ONNS Defragmentation Tool Concepts" (p. 34-2)

Before you begin

This task requires you to have the appropriate NE documentation at hand.

The ONNS Defragmentation command line tool can be executed while the OMS application is up and running. You must have an **oms** login to execute this tool.

Task

Complete the following steps to insert an Optical Network Navigator System (ONNS) node in an active ONNS Network

1 After **Internal Network** ports on both sides of the link where the new node is to be inserted are set to lockout, verify that OMS also reflects this portControl setting.

2 For each connection that is riding on the internal network link, roll the connection away from the link using the documented procedures.

In OMS, verify that these connections are now marked **Stale** and that the layout reflects the network.

On the NE, if an empty port operation is performed to remove the connections, verify that the defragmentation script is run in OMS to mark the connections as **Stale**.

Delete MxN connections from OMS. (They cannot be moved.)

3 From the NE management functions of the OMS GUI, disable the SCN and DCN on the internal network link. Verify that the NE still has other links that have SCN and DCN enabled.

4 Re-provision any **Internal Network** ports as **Customer/Client** ports. Verify that OMS reflects this re-provisioning.

5 Using the NE documentation, disconnect and reconnect the appropriate fibers with the new ONNS node inserted.

6 Once the ports have been reset to **Internal Network**, verify that OMS reflects the same.

7 Once DCN and SCN are re-enabled on these two new links, OMS needs to inventory these links via a database synchronization process.

8 If the original connections are rolled back, verify that OMS marks these connections as **Stale** and that the layout reflects the network.

END OF STEPS

Replace Controller Units for CMISE NEs

When to use

Use this task to replace a controller unit circuit pack (the pack) in a CMISE NE when the replacement pack might already contain a Management Information Database (MIB). This task allows you to decide to accept the MIB in the OMS or to use the MIB that is present in the new controller card.

Important! If there is no MIB in the new controller card or if you are uncertain of the contents of the MIB, you must perform a MIB download at Step 5 to use the MIB that is currently in OMS.

Related information

See the following topic in this document:

- "Summary of supported NEs" (p. 1-5)

Before you begin

Carefully check the new controller circuit pack to determine the following:

- if it contains the correct software version
- if it is the same type as the old controller circuit pack

Task

Use this task to replace a controller unit in a CMISE NE when the replacement controller unit might already contain a database MIB.

1 From the management system GUI, disable the association between the OMS management system and the NE by accessing the NE Management Functions page and performing a MIB download to the selected NE by selecting the **Manage MIB** function in the **Network Element** category.

2 Remove the circuit pack from the NE.

3 Insert another circuit pack into the NE that has a valid MIB.

Result: The NE starts.

4 On the management system GUI, access the **OMS to NE Connections** page and change the Network Service Access Point (NSAP) address for the NE to reflect the NSAP address of the newly inserted circuit pack.

5 On the management system GUI, access the **NE Management Functions** page and do either one of the following:

- Perform a MIB download to the selected NE to align the MIB in the NE to the one in the OMS
- Perform a MIB upload to the selected NE to align the MIB in the OMS to the MIB in the NE and go to Step 6.

6 After the operation is complete, if a MIB upload was performed, perform a full database synchronization from the management system GUI:

Tools > DB Synchronization

END OF STEPS

Run the Nagios Tool

When to use

Nagios tool helps manage the network, which includes salient features like displaying the number of available licenses, viewing the number of logged in users, and viewing the load sharing of OMS GUI servers. This script replaces the webadm - c Users. The two scripts included in Nagios tool to manage a network are:

`viewLoggedInUser`

This script captures and displays the Users logged into the OMS server. The logged in User information is displayed in a specified format.

`check_license[-nf]`

This script determines the number of remaining licenses for each NE type. When the option **-n** is used, the script checks the NE type model licence.When the option **-f** is used, the script prints the output in a specified format.

Related Information

This task does not have any related information.

Before you begin

This task does not have any preconditions.

Task

Use this task to view the number of available licenses, number of logged in users, and the load sharing of OMS GUI servers.

1 Run viewLoggedInUsers

Result: The number of Users logged into the OMS server is displayed.

2 Run check_license [-n].

Result: The NE type model licence is displayed.

3 Run check_license [-f]

Result: The output is printed in a specified format.

END OF STEPS

Appendix A: Tool Summary

Overview

Scripts and Tools

OMS provides users with a complete list of UNIX-based tools that can be used to ease many repetitive tasks. These tools are executed from the UNIX command line of the system console (of the Server Platform or the PC Platform) on which the management current resides and is running.

Summary

Tool	Location	Platform and License	Used to...
astn_defrag	Chapter 34, “ONNS ”	Server and PC Platforms “OMS_CORE license” (p. 5-5)	Identify connections that have could have been impacted by a defrag on the NE CIT.
AutoDiscover	Chapter 22, “Connection Auto Discovery”	Server and PC Platforms “OMS_CORE license” (p. 5-5)	Discover connections that terminate on and pass through NEs under OMS control.
bulk_DBdelete	Chapter 39, “Bulk Database Delete”	Server and PC Platforms “OMS_CORE license” (p. 5-5)	Bulk delete connections/multiplex sections in the database.
CNA_mib_transform **CNA_restore_nes**	Chapter 29, “CMISE NE Database Conversion”	Server and PC Platforms “OMS_CORE license” (p. 5-5)	Manipulate the MIB on a CMISE NE.
DataExtraction	Chapter 16, “Data Extraction”	Server Platform “OMS_DET license” (p. 5-6)	Extract equipment, alarm, NE, network connection, PM, and for certain NEs, link connection data, from OMS.
ea_import_bb_nes	Chapter 35, “Non-managed NEs”	Server and PC Platforms “OMS_CORE license” (p. 5-5)	Bulk add non-managed NEs to OMS.

Tool	Location	Platform and License	Used to...
ept_route_id_update	Chapter 33, "EPT Route ID Update"	Server Platform "OMS_CORE license" (p. 5-5)	Update the route ID for in-effect existing and pending LambdaXtreme™ Transport connections in the NRM and OMS databases using EPT generated route ID values.
lt_cron_admin	Chapter 22, "Connection Auto Discovery"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Schedule the automatic execution of tools such as **AutoDiscover.**
LXChannelUpgrade	Chapter 27, "LambdaXtreme® Channel Upgrade"	Server Platform only "OMS_CORE license" (p. 5-5)	Upgrade the number of channels from 64 to 128 when the 1625 LambdaXtreme® Transport version is upgraded from R6.0 to R7.0 within the managed domain.
LXNodeUpgrade **merge_node**	Chapter 26, " 1625 LambdaXtreme® Transport DWDM Upgrade and Merge"	Server Platform "OMS_CORE license" (p. 5-5)	Upgrade existing 1D_ROADM and 2D_ROADM DWDM 1625 LambdaXtreme® Transport NEs to 3D_WXC NEs and merge them into one WXC system NE.
NEInServiceUpgrade	Chapter 25, "NE In-Service Upgrade"	Server Platform "OMS_CORE license" (p. 5-5)	Accommodate the generation of LCs and contained TPs based on the interface standard of a particular 1675 Lambda Unite MultiService Switch (MSS) circuit pack.
ne_name_change	Chapter 31, "NE Name Change"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Rename the names of managed, non-managed, or unknown NEs.
ne_reparent	Chapter 32, "NE Reparenting"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Move one or more CMISE NEs from an ITM-SC R11.4.3 managed network to a CNA managed network.
network_inventory_extraction	Chapter 23, "Network Inventory Extraction"	Server Platform "OMS_NETINV license" (p. 5-12)	Map OMS data elements to VPIsystems™ format and extract that data from the OMS database for ONNS/ASTN use.

Tool	Location	Platform and License	Used to...
OmsBulkUpld	Chapter 38, "Bulk Upload of Digital Link and Connections"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Bulk upload a digital link and connections to OMS or bulk provision a digital link and connections to OMS.
OmsInsertNode	Chapter 24, " Insert/Remove Node"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Insert an NE into a ring/multiplex section connection.
OmsLoadX	Chapter 35, "Non-managed NEs"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Modify cross-connections in non-managed NEs.
OmsModifyConnParams	Chapter 36, "Bulk Renaming of Connections"	Server and PC Platform "OMS_CORE license" (p. 5-5)	Rename connection names that were generated through path discovery to actual connection names.
OmsModifyEthernet-Params	Chapter 37, "Ethernet"	ServerPlatforms "OMS_CORE license" (p. 5-5)	Rename Ethernet services names that were generated through Ethernet resynchronization to actual Ethernet service names.
OmsRemoveNode	Chapter 24, " Insert/Remove Node"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Remove an NE from a ring/multiplex section connection.
TDMOpticalLinesUp-grade	Chapter 28, "TDM NE Optical Lines Upgrade"	Server and PC Platforms "OMS_CORE license" (p. 5-5)	Upgrade optical lines within the managed domain for TDM directly managed NEs, NEs that are managed through a legacy EMS, and black boxes.

Index